TELKOMNIKA Telecommunication Computing Electronics and Control
Vol. 22, No. 3, June 2024, pp. 499~509
ISSN: 1693-6930, DOI: 10.12928/TELKOMNIKA.v22i3.25896

Multi-stage cryptography technique for wireless networks

Amer Alsaraira[1], Samer Alabed[1], Omar Saraereh[2]
[1]Department of Biomedical Engineering, School of Applied Medical Sciences, German Jordanian University, Amman, Jordan
[2]Department of Electrical Engineering, Faculty of Engineering, The Hashemite University, Zarqa, Jordan

Article Info

Article history:

Received Dec 4, 2023
Revised Jan 5, 2024
Accepted Jan 19, 2024

Keywords:

Cryptography
Cyber physical system
Digitalization
Internet of things
Secure communication system
Smart cities
Sustainability

ABSTRACT

The security of wireless communication systems has been the focal subject of research for more than a century. It is a topic of vital importance due to its effectiveness in many fields. Besides, the importance of sending data from one point to another without intercepting by unwanted third-party has become an essential requirement in conjunction with the widespread hacking technologies. This research paper is set out to explore a new technique used in internet of things applications that will ensure a secure wireless communication system. Additionally, it clarifies five distinct cryptographic methods: advanced encryption standard, elliptic curve cryptography, transposition, substitution, and Rivest, Shamir, and Adleman. In addition, the secure wireless communication system combines four of the prementioned techniques to build a highly secure system. Moreover, we managed to elucidate the critical points of our work on the long-range systems into a short yet informative and detailed summary. This paper will extensively cover the following topics: cryptography, cryptographic methods and techniques, software implementation, applications, and advantages of the system.

Corresponding Author:

Amer Alsaraira
Department of Biomedical Engineering, School of Applied Medical Sciences
German Jordanian University
Amman-11180, Jordan
Email: amer.alsaraira@gju.edu.jo

1. INTRODUCTION

The need for new wireless technologies is going up because we depend on wireless connections more and more. People and businesses need faster and more secure wireless solutions. New wireless technologies are really needed because they can make our connections even better [1]-[4]. These new technologies can help make our connections more secure and protect them from cyber threats. With more devices connected to the internet, it is important to have strong wireless technologies to keep them safe. So, as the world gets more connected, we need the latest wireless technologies not just for better connections but also to keep our networks secure from hackers and bad things. Cyber-attacks have developed over the years. On that account, network security faces challenges to protect communication systems. Previous studies have reported fluctuations in security systems that include encoded data. Attackers can literally identify the used types of encodings and ciphers by online free tools. These tools facilitated the attacking process, in which data are placed in a critical position, as a result hackers can crack and reveal the content of this transmitted data.

This paper seeks to tackle this problem by introducing a new approach that will accomplish two main things: security and transmitting data over a long-distances using radio signals. The secure wireless communication system (SWCS) provides a new vision in the world of communication which will secure the process of transmitting messages over a long range. Furthermore, this work could be used in many applications, including military, healthcare, education, civilian, internet of things (IoT), and emergency, without requiring towers or internet coverage. The most striking part of this work is it is ability to provide connectivity to dead areas and its complete dependency on radio signals using long range wide area network (LoRaWAN), which eliminates the usage of satellites, internet coverage, and Bluetooth. The software implementation of this work emphasizes cryptography and introduces the novel method. Thus, this work meets a wide range of criteria, including affordability, power efficiency, usability, indoor penetration, and level of protection.

2. CRYPTOGRAPHY

By converting data into an unreadable format using cryptographic methods and procedures developed from arithmetic and a set of algorithm principles cryptography is the discipline concerned with safeguarding data from unauthorized access [5]-[7]. The term 'cryptography' is derived from Greek, with 'Krypto' signifying 'secret' and 'Graphein' denoting 'message'," were combined to form the English word "cryptography" [6], [8]. Taking this a step further, encryption and decryption might be used to create cryptography. The act of converting plaintext into cipher text is known as encryption [5], [6], [8]. Decryption, on the other hand, is the process of restoring cipher text to its original form. A secret key, commonly referred to as a password, is also required in order to decrypt the message and reveal it is encrypted information. Under different circumstances, the message remains inaccessible unless an unauthorized individual breaches the system. The primary objective of cryptography is to secure sensitive data through the utilization of unintelligible text, which can only be deciphered by authorized recipients possessing a shared key. Cryptography is often described as the 'art of secrecy' due to it is role in shielding critical information from external threats and maintaining it is high level of security [9]-[14]. Cryptography keys can be classified into two primary categories: symmetric keys and asymmetric keys. Symmetric key encryption, sometimes called private key encryption, entails generating a solitary private key shared exclusively among authorized parties. This exclusive key ensures that only those with access to it can decipher the message, while others are unable to do so [6]-[9]. Distinguished instances of symmetric key algorithms encompass the advanced encryption standard (AES), Blowfish, and the data encryption standard (DES) [9]. In contrast, asymmetric keys utilize a pair of keys: a private key for encryption and a public key for decryption of the plaintext. The public key is accessible to everyone, while the private key must be kept confidential to ensure that only the designated recipient can decrypt the ciphertext. This reversible method allows two parties to communicate, with one employing the public key for encryption and the other using the private key for decryption. Another term for this approach is public key encryption. Examples of asymmetric encryption methods include the elliptic curve cryptosystem (ECC) and the Rivest, Shamir, Adleman (RSA) system [9].

2.1. Symmetric encryption

Symmetric encryption uses the same private key to encrypt plaintext by employing letters, numerals, and symbols that have been altered using one or more symmetrical encryption algorithms [7], [9], [11]-[14]. The recipient and sender then exchange a private key, as seen in Figure 1, which is then used to decrypt the cipher text. The symmetric key performs better than asymmetric methods [9].

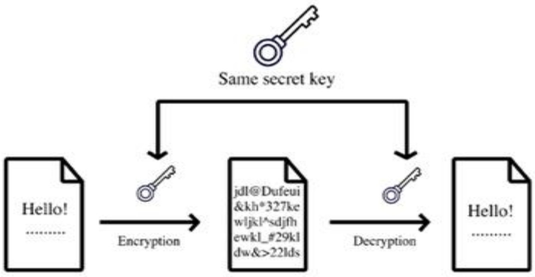


Figure 1. Symmetric encryption

2.1.1. Advanced encryption standard

The AES is a symmetric encryption key known for its robust data protection capabilities. It gained widespread recognition due to its strength in safeguarding information. In 1997 by the national institute of standards and technology (NIST), AES was created with the aim of rectifying the weaknesses found in DES. DES had become obsolete due to its short key length, which made it susceptible to rapid compromise.

Consequently, DES is no longer considered a viable solution for data protection. In contrast, AES was introduced to ensure high levels of security and was formally adopted as a federal standard on November 26, 2001. Notably, the AES algorithm is characterized by it is versatility, as it supports various key lengths, including 128, 192, and 256 bits, with corresponding numbers of rounds (10, 12, and 14) [15]. The AES algorithm comprises three main layers, each dedicated to performing specific mathematical operations, as illustrated in Figure 2.

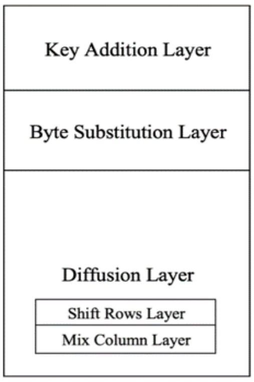
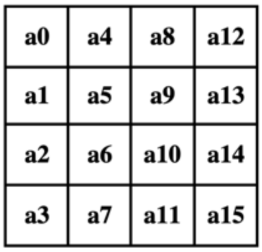


Figure 2. AES architecture

Brief description of each layer [13]:

- Key addition layer: both the 128-bit key and the user's plain text (also known as the state) are structured in a 4×4 matrix as illustrated in Figure 3. Each key consists of round keys. As a rule, each round at the beginning will perform a logical exculsive OR (XOR) on the plain text with the 128-bit key. Assuming AES-128 bit, it means the encryption and decryption process will go through 10 round keys. Every round consists of four stages: byte substitution, row shifting, column mixing, and the addition of a round key. The nine rounds encompass all phases, with the exception of the tenth round, where the column mixing phase is excluded.
- Layer of byte substitution: as suggested by its title, this layer employs a non-linear substitution process using a lookup table, supported by distinct mathematical characteristics. In this application, all the 16 bytes of the state (input) are substituted by its corresponding value in the S-box table.
- Diffusion layer: this layer comprises two sublayers-row shifting and column mixing, both of which execute linear operations, as opposed to the non-linear byte substitution layer [13].
- Shift rows layer: the shift rows layer performs a simple permutation. The rows in the matrix will cyclically shift, excluding the first row. Starting from the second row, the first element in the state matrix is shifted by a one-byte position to the left, the third row by two-byte positions, and the fourth row by three-byte positions. Figure 4 elucidates the shift rows phase.
- Mix columns layer: in contrast with the shift rows, the mix columns layer manipulates the state columns in which a multiplication operation is executed along with Galois field operations.

The decryption process will take the inverse of each layer to unlock the encoded message. Figure 5 illustrates the process.



a0	a4	a8	a12
a1	a5	a9	a13
a2	a6	a10	a14
a3	a7	a11	a15

Figure 3. Four by four plain-text matrix

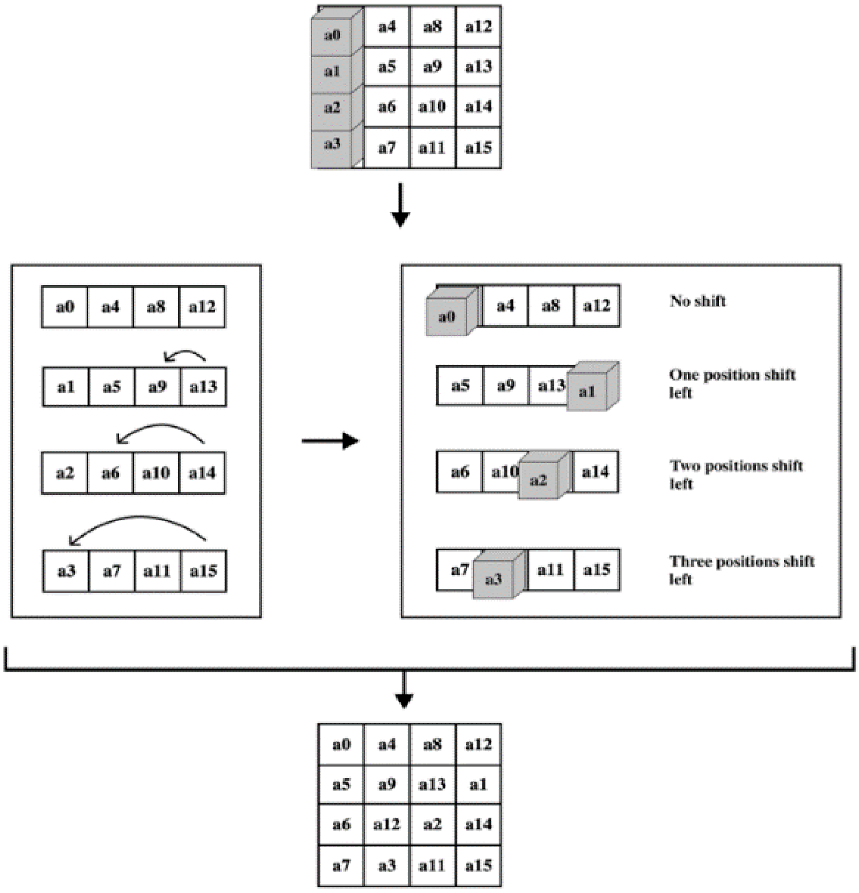


Figure 4. Shift rows phase

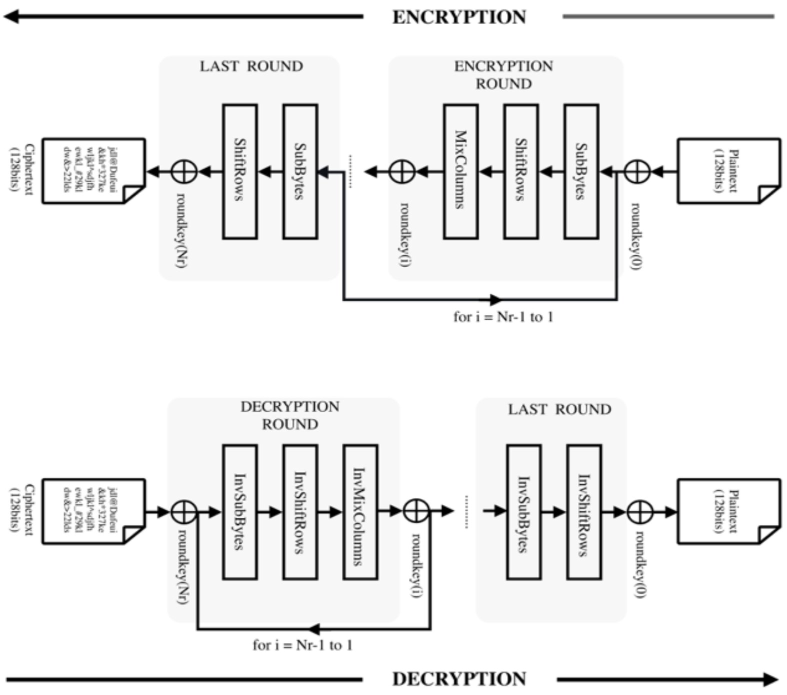
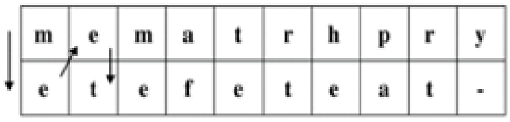


Figure 5. AES encryption and decryption process

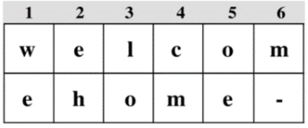
2.1.2. Transposition

One of symmetric cryptographic algorithms is the transposition algorithm. It depends on converting the plain text into cipher text by rearranging the order of the elements in the plain text [5]. The transposition algorithm encompasses a range of methods, including the Rail Fence and the simple columnar transposition techniques. Rail Fence: in this technique, the plain text is written diagonally then is read as a series of rows [5]. For example: assuming the following plain text: “meet me after the party” it will be written diagonally as shown in Figure 6. To create the ciphertext, the process involves taking each element in Figure 6 from left to right and then reading it sequentially, row by row. This results in the following ciphertext: ‘mematrhpryetefeteat’. In the case of the Simple Columnar technique, the plain text is organized in a rectangular format, with rows written sequentially and subsequent reading of data performed column by column. It is essential to establish the precise dimensions of this rectangular arrangement, and it is equally vital for both the sender and the recipient to be knowledgeable about the key that dictates the reordering of the columns within the rectangle [5], [6]. For example, assume the following plain text: “welcome home”, key: ZEBRAS, order: 632415. To produce the cipher text, we must read it column by column according to the defined order as shown in Figure 7. In the example above, the plain text will produce the following cipher text: “mloehcmweoe”.



m	e	m	a	t	r	h	p	r	y
e	t	e	f	e	t	e	a	t	-

Figure 6. Transposition process



1	2	3	4	5	6
w	e	l	c	o	m
e	h	o	m	e	-

Figure 7. Generating cipher text using the key order

2.1.3. Substitution

The substitution method is just one of numerous cryptographic approaches. It is primary function is to transform plain text into ciphertext through encryption and reverse this process by converting ciphertext back into plain text through decryption. This transformation involves replacing individual characters or character groups with alternate ones. In this method, a letter table is employed. In Figure 8, the first row displays letters arranged in alphabetical order, while the second row is organized in a cryptographic sequence. Occasionally, the letter arrangement may be influenced by a shared key between the sender and receiver. Consequently, both the sender and receiver need to possess an identical table to facilitate the encryption and decryption of messages.

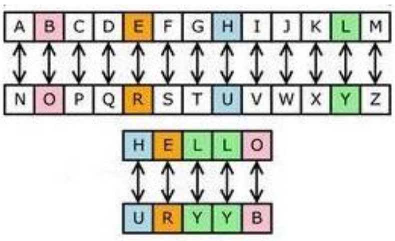
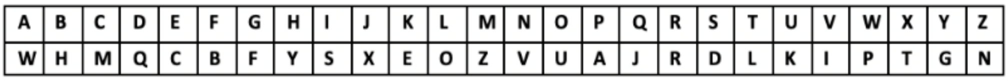


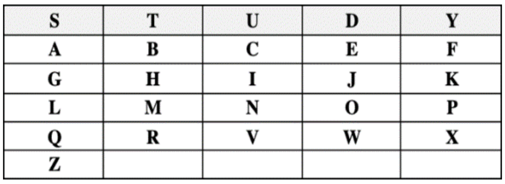
Figure 8. Substitution table example

Example 1: using Figure 9, the plaintext into ciphertext by replacing the characters in the first row with their corresponding counterparts in the second row. For instance, change ‘G’ to ‘F,’ ‘R’ to ‘R,’ ‘O’ to ‘U,’ and ‘P’ to ‘A.’ As a result, the ciphertext becomes (FRUKA). Example 2: This example illustrates the arrangement of alphabetic characters based on a predetermined key. If we take the key ‘STUDY,’ the cryptographic character order is established by placing the key in the first row, as depicted in Figure 10. Subsequently, the remaining characters, excluding those from the key, are inserted into the following rows in a sequential manner. Next, the substitutional table will be built depending on the reading technique of the above characters. For this example, shown in Figure 11. The characters will be sequentially taken from each column to create the cipher table. Hence, when the plaintext is ‘HELLO,’ the ciphertext, as indicated in Figure 12, will be “BQUUN”.

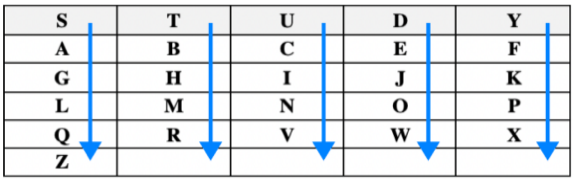


A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
W	H	M	Q	C	B	F	Y	S	X	E	O	Z	V	U	A	J	R	D	L	K	I	P	T	G	N

Figure 9. Substitution table

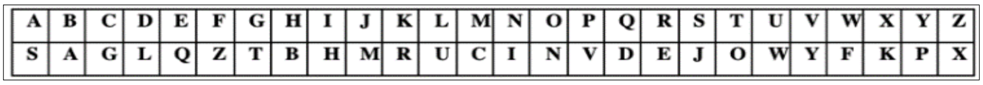


S	T	U	D	Y
A	B	C	E	F
G	H	I	J	K
L	M	N	O	P
Q	R	V	W	X
Z				



S	T	U	D	Y
A	B	C	E	F
G	H	I	J	K
L	M	N	O	P
Q	R	V	W	X
Z				

Figure 10. Excluding the key characters Figure 11. The procedure for creating the cipher table



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
S	A	G	L	Q	Z	T	B	H	M	R	U	C	I	N	V	D	E	J	O	W	Y	F	K	P	X

Figure 12. Cipher table

2.2. Asymmetric encryption

Asymmetric key encryption, as was previously noted, requires two keys: a public key for encryption and a private key for decryption as shown in Figure 13. RSA is one of the most well-known asymmetric cryptographic examples. Numerous researchers accepted the RSA method and strongly supported it as the most widely used and well-known one. However, asymmetric encryption not only embraces RSA but also ECC algorithm that came to the life after 8 years of inventing RSA.

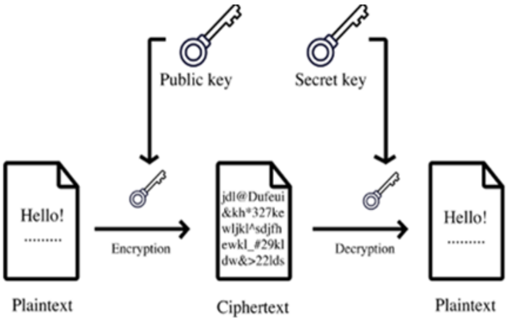


Figure 13. Asymmetric encryption

2.2.1. Rivest, Shamir, Adleman

RSA is a type of asymmetric encryption algorithms that was invented in 1977 and named after three scientists: R. Rivest, A. Shamir, and L. Adleman [16]-[18]. RSA algorithm is centered on the difference between finding two large prime numbers easily and the difficulty of factoring the primes' product [18]. Nevertheless, the advancement of computer technology over time has simplified the process of factoring large prime numbers, thereby making RSA vulnerable to attacks. In RSA, a public key is used to encrypt the plain text to produce a cipher text, compared with the decryption procedure which is done through a private key as shown in Figure 14. To perform encryption and decryption using RSA, both the public key, accessible to everyone within the network, and the private key, maintained in secrecy and known to the intended recipient, are employed. The RSA algorithm encompasses two primary components: key generation and RSA encryption [16], [17].

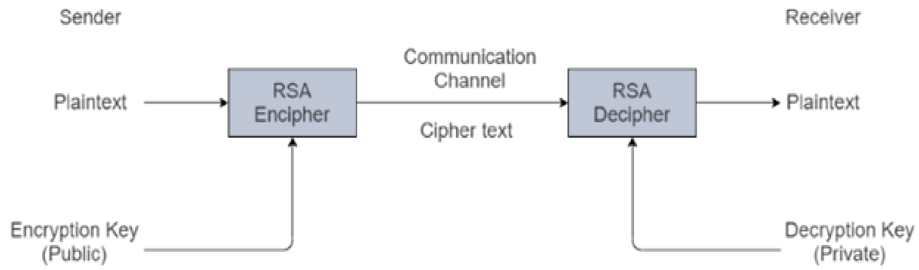


Figure 14. The process of RSA

2.2.2. Elliptic curve cryptography

In 1985, ECC was initially introduced to the cryptographic universe by Neal Koblitz and Victor Miller [19], [20]. ECC is relatively considered as a new asymmetric or public-key cryptographic system. It is considered an intense competitor of digital signature algorithm (DSA) and RSA cryptographic systems. Since any crypto-system relies mainly on the complexity level of the applied mathematical equations, a higher difficulty level yields better security. Scientists introduced two algorithms to analyze mathematical problems, polynomial and exponential. These two algorithms are used to analyze the difficulty level of any cryptosystem's algorithms where complicated equations equate with exponential and easy ones with polynomial [21]. It was found that the best algorithm formed so far to solve the hard mathematical problems in ECC takes full exponential time. On the other hand, other techniques such as RSA and DSA take sub-exponential time. Based on that, ECC can achieve a higher security level with fewer parameters compared with RSA and DSA [19]-[23]. For example, for an ECC system to have the same security as 1,024-bit RSA or DSA system, it will require only 160-bit [21]-[23]. ECC could be implemented either using a discrete logarithm problem or by using points on an elliptic curve. Figure 15 shows two elliptic curves resulting from substituting different values in (1) and (2):

$$y^2 = x^3 + ax + b \quad (1)$$

$$4a^3 + 24b^2 \neq 0 \quad (2)$$

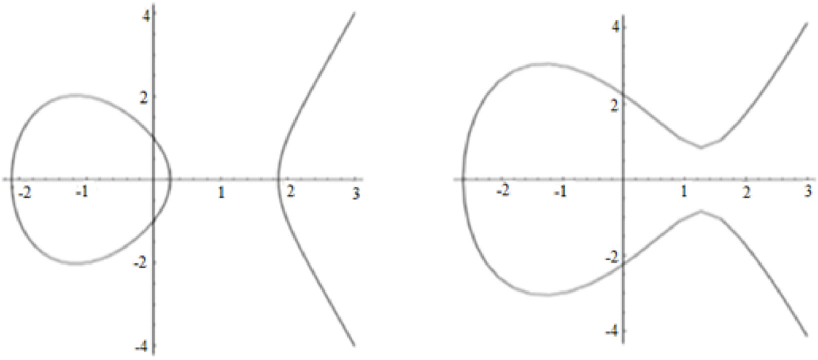


Figure 15. Elliptic curves graphs. On the left, y2=x3−4x+1 and on the right y2=x3−5x+5 [21]

Pursuing this further, by using the scale point multiplication of a starting point on an elliptic graph (P) and a positive integer value (k) as in k.P, this will result in a new point on the elliptic curve and will repeated the process n times, which is the private key value. Moving to the implementation of ECC using discrete logarithmic problems, with the aid of (1), a point on the curve can be generated by substituting a and b in (1) and (2). To keep the results in a finite field, the equation has to get multiplied by the modulus of P. After that, a point on the elliptic curve will be chosen and added to itself n times, where n is the private key. The point chosen on the elliptic curve has to be delicately chosen such that when added to itself multiple times generates as many new points as possible before going in a loop of pre-generated points. In general, a very extensive literature has analyzed several approaches using an elliptic curve in securing data [21]-[25].

3. SOFTWARE IMPLEMENTATION

Among a multitude of cryptographic ciphers, none of them was strong enough to shield data. As soon as the cipher technique is identified or vulnerability is discovered, the system becomes fragile to intruders. Since the current ciphers are predictable and crackable, it becomes a must to at least ensure high protection. Broadly speaking, the secure wireless communication system is built to achieve protection, which envelops data using a special combination of symmetric and asymmetric algorithms. Accordingly, among various algorithms, the four system bones which were chosen to manipulate data are AES, transposition, substitution, and ECC as shown in Figure 16. Without further a due, lets expand the new approach:

a. Initially, each crypto system is sorted by listing them in a scale of 1 to 4.
b. Set the private key to be 16 characters as shown in Figure 17.
c. Then, the first four characters will be selected and sorted in an ascending order as shown in Figure 18.

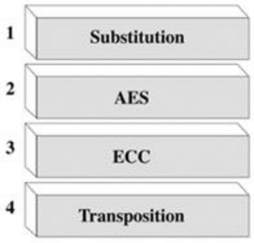
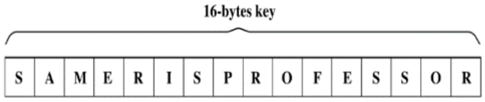


Figure 16. Sorting the chosen techniques



S	A	M	E	R	I	S	P	R	O	F	E	S	S	O	R

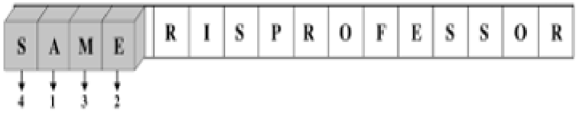


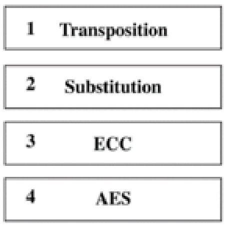
Figure 17. A private key consisting of 16 bytes

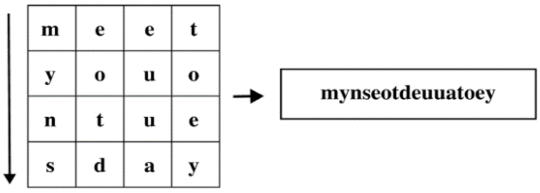
Figure 18. Selecting the first four bytes

The idea behind this is to execute each layer based on the order of the first four characters in the private key, which constantly changes if the private key changed. By this approach, it will be unlikely to crack the system because it produces a sort of a puzzle each time a new key is generated. When generating a new key, new layers arrangement will be executed. According to the predefined numbers given to the above cryptographic techniques in step 1, the execution of each layer will be as shown in Figure 19.

d. Let's consider the sender's original message: 'Meet you on Tuesday'. To initiate the transport layer, following the principles outlined in the transposition section, all the characters in the plaintext will be organized into a 4×4 matrix. However, a distinctive aspect of this technique is that the matrix reading pattern will be determined by the initial character in the encryption key, as explained:
   - If the key begins with a letter, the ciphertext will be read column by column.
   - If the key commences with a number, the ciphertext will be read from right to left.
   - If the key starts with a specific character, the ciphertext will be read in a zigzag pattern.

   Since the key starts with a letter in the example, the output of this layer will produce the following cipher text as shown in Figure 20.





m	e	e	t
y	o	u	o
n	t	u	e
s	d	a	y

mynseotdeuuatoey

Figure 19. Reordering based on the private key

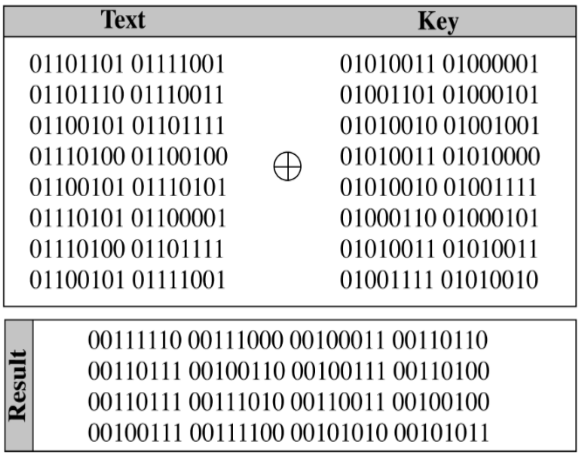
Figure 20. Transposition implementation

e. Next, the generated output of step 4 will be taken as an input for the substitution layer. For this application, each character in the text and key will be converted to its equalized ASCII binary format:
Text: mynseotdeuuatoey
Binary format:
01101101 01111001 01101110 01110011 01100101 01101111 01110100 01100100 01100101 01110101 01110101 01100001 01110100 01101111 01100101 01111001
Key: SAMERISPROFESSOR
Binary format:
01010011 01000001 01001101 01000101 01010010 01001001 01010011 01010000 01010010 01001111 01000110 01000101 01010011 01010011 01001111 01010010
Next, performing an XOR operation between the text and the key, as illustrated in Figure 21, results in the subsequent ciphertext: >8#67&'47:3$'<*+

f. Then, ECC will be applied to the previous outputted cipher text generating the new following cipher:
MEYCIQDCauxvGgR+caJrNGz2KUsaEN1ZMGUiUXVd+wPdeSQtHgIhAOgjygKtotxe7pte4BOuwj0WnXKdOAHGsbwxs0TyKhww

g. Finally, AES will be executed producing:
SyiRmN5ujcVaBxa70fc0CYLiAzC/CmaTZii4bAqeOLo4RhAqsbAo2uJ4nYm/tFCNfxVGaOCSa77EFAjlVwQYhxPEKcQdmOMHJlKtUWzlN2pYZICH4DV9iXZW8WioBPGHvLuMfV9GuVuzoxiMH5kh3Q==

Accordingly, the plaintext “meetyouontuesday” that the sender sent to the receiver, with respect to the key “SAMERISPROFESSOR”, will be received by any recipients as the next cipher text: “SyiRmN5ujcVaBxa70fc0CYLiAzC/CmaTZii4bAqeOLo4RhAqsbAo2uJ4nYm/tFCNfxVGaOCSa77EFAjlVwQYhxPEKcQdmOMHJlKtUWzlN2pYZICH4DV9iXZW8WioBPGHvLuMfV9GuVuzoxiMH5kh3Q==”. The previous four steps can be summarized as shown in Figure 22.



Text		Key
01101101 01111001		01010011 01000001
01101110 01110011		01001101 01000101
01100101 01101111		01010010 01001001
01110100 01100100	⊕	01010011 01010000
01100101 01110101		01010010 01001111
01110101 01100001		01000110 01000101
01110100 01101111		01010011 01010011
01100101 01111001		01001111 01010010

Result	00111110 00111000 00100011 00110110
	00110111 00100110 00100111 00110100
	00110111 00111010 00110011 00100100
	00100111 00111100 00101010 00101011

Figure 21. Conducting a logical XOR operation between the plaintext and the key

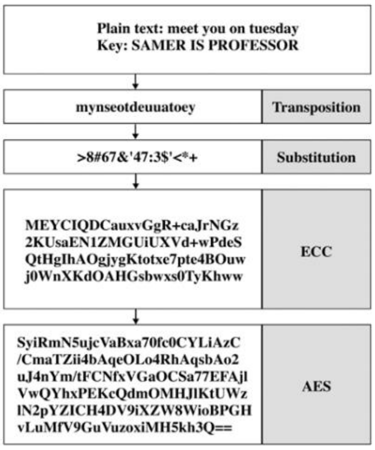

Plain text: meet you on tuesday
Key: SAMER IS PROFESSOR
mynseotdeuuatoey
Transposition
>8#67&'47:3$'<*+
Substitution
MEYCIQDCauxvGgR+caJrNGz2KUsaEN1ZMGUiUXVd+wPdeSQtHgIhAOgjygKtotxe7pte4BOuwj0WnXKdOAHGsbwxs0TyKhww
ECC
SyiRmN5ujcVaBxa70fc0CYLiAzC/CmaTZii4bAqeOLo4RhAqsbAo2uJ4nYm/tFCNfxVGaOCSa77EFAjlVwQYhxPEKcQdmOMHJlKtUWzlN2pYZICH4DV9iXZW8WioBPGHvLuMfV9GuVuzoxiMH5kh3Q==
AES

Figure 22. The process of the security system

4. IMPORTANCE AND APPLICATION

This project compiles security and transceiver. Hence, it can be used in several delicate applications since security is the innermost ring of the system. Moreover, data can be transferred safely over a long-range using radio frequency signals. This code can be used on LORA systems in order not to need coverage, mobile phone operators, or satellite signals. It should be noted that this system implementation requires a very low budget to be produced. Consequently, there are countless applications of such a system. Some of these applications are as follows:

a. It can be mounted on a drone or a robot to send and receive data or control signals across a long distance. It is applicable for both military and civilian districts such as:
   - Oil and gas industry: to inspect remote and high-risk regions, fields, and pipelines.
   - Electric utility companies: to inspect power lines.
   - Army: get a high-ground picture of dangerous areas, or safely manoeuvre through a minefield.
   - Education establishments and many other companies.

b. By using it, an efficient mobile phone system can be established without the need for any type of internet or wireless coverage. This is because it will not require any subscription identity module (SIM) card. It can be used as a communication channel to receive and send text messages, images, data signals, information, and control signals for countless military and civilian sectors such as:
   - The oil and gas industry: to establish a long-distance connection between workers in rural locations.
   - Army: to provide a highly secure connection between soldiers and commanders in war and peace.
   - In an emergency or to relieve stress, you can send data and messages if there is no coverage.
   - Non-military use cases: affordable local telephone services.
   - Banking, academic, and private sectors: to create a safe relationship amongst staff members.
   - Create notification systems and offer a wide range of services to numerous additional industries.

c. Establish a reliable and secure healthcare system capable of operating across extensive distances, independently of SIM cards, internet connectivity, or radio frequency coverage for data and information transmission. Furthermore, integrate various sensors into the system, including temperature, and biomedical sensors, to promptly notify healthcare professionals of any unexpected health changes or deteriorations in patients.

d. It has the potential to save numerous lives by identifying accidents and promptly relaying the accident's location to the nearest emergency facility.

e. It is useful for creating effective internet of things systems. The system will only need a minimal amount of energy thanks to solar panels.

f. It can be applied to social media, satellite applications, and wireless networks.

5. CONCLUSION

To sum up, the security of wireless communication systems has received significant attention and development over many centuries. It has been developed successfully based on two aspects: security and long-range communication. Furthermore, LoRa has been used as a primary component due to its marvellous features in transmitting and receiving data over long-range and employing free frequency bands. Likewise, the solar panel has been used to power up the microcontroller. Correspondingly, the SWCS has many advantages and covers many criteria, such as low power consumption, low cost, and ease of use. This research paper aims to remedy the common problem of less security in sending and receiving data. A full explanation of various encryption and decryption techniques has been discussed in detail. The techniques covered in this paper are substitution techniques, transposition techniques, RSA techniques, AES and ECC techniques. In addition to cryptographic methods and techniques explanation, software implementation, applications, and advantages of the system have been discussed.

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.icte.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 *Proceedings of 19th International ITG Workshop on Smart Antennas, WSA 2015,* 2015.

[3] X. Shen, H. Li, Y. Wang, Z. Wei, Z. Feng, and Z. Wang, "A feasibility study on integrated sensing and communication in cooperative network," in *2022 31st Wireless and Optical Communications Conference (WOCC)*, Aug. 2022, pp. 80–84, doi: 10.1109/WOCC55104.2022.9880583.

[4] S. Alabed, M. Pesavento, and A. Klein, "Distributed differential space-time coding for two-way relay networks using analog network coding," in *European Signal Processing Conference*, 2013.

[5] B. Schneier, *Applied cryptography: protocols, algorithms, and source code in C,* vol. 10, no. 5. John Wiley and Sons, 2007.

[6] W. Stallings, "Cryptography and network security: principles and practice," *Person Education Inc*, p. 752, 2016.

[7] C. Paar and J. Pelzl, *Understanding cryptography: a textbook for students and practitioners*, 2nd ed. Springer, 2010.

[8] A. Krishna A and L. C. Manikandan, "A study on cryptographic techniques," in *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 2020, pp. 321–327, doi: 10.32628/cseit206453.

[9] A. J. Menezes, P. C. V. Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. 1996.

[10] A. Yeboah-Ofori, C. K. Agbodza, F. A. Opoku-Boateng, I. Darvishi, and F. Sbai, "Applied cryptography in network systems security for cyberattack prevention," in *2021 International Conference on Cyber Security and Internet of Things (ICSIoT),* Dec. 2021, pp. 43–48, doi: 10.1109/ICSIoT55070.2021.00017.

[11] A. Srivastava, H. Pandey, A. Kumar, and M. Poonia, "Enhanced hybrid symmetric cryptography for IoT devices," in *2022 IEEE Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI)*, Dec. 2022, pp. 1–4, doi: 10.1109/IATMSI56455.2022.10119338.

[12] D. K. Sharma, N. C. Singh, D. A. Noola, A. N. Doss, and J. Sivakumar, "A review on various cryptographic techniques and algorithms," *Materials Today: Proceedings*, vol. 51, pp. 104–109, 2021, doi: 10.1016/j.matpr.2021.04.583.

[13] G. C. Kessler, "Introduction to cryptography." Embry-Riddle Aeronautical University, 2012.

[14] J. Ma, "Basic application of mathematics in cryptography," in *2020 International Conference on Modern Education and Information Management (ICMEIM),* Sep. 2020, pp. 871–875, doi: 10.1109/ICMEIM51375.2020.00192.

[15] S. S. S. Priya, M. Junias, S. S. Jenifer, and A. Lavanya, “Implementation of efficient mix column transformation for AES encryption,” in *Proceedings of the 4th International Conference on Devices, Circuits and Systems, ICDCS 2018*, 2019, pp. 95–100, doi: 10.1109/ICDCSyst.2018.8605077.

[16] S. K. Singh, P. K. Manjhi, and R. K. Tiwari, “Data security using RSA algorithm in cloud computing,” *Ijarcce*, vol. 5, no. 8, pp. 11–16, 2016.

[17] M. A. Taha and M. Farajallah, “Survey paper: cryptography is the science of information security,” *International Journal of Computer Science and Security (IJCSS)*, no. 5, pp. 298–309, 2011.

[18] M. Preetha and M. Nithya, “A study and performance analysis of Rsa algorithm,” *Ijcsmc*, vol. 2, no. 6, pp. 126–139, 2013.

[19] J. VenkataGiri and A. Murty, “Elliptical curve cryptography design principles,” in *2021 International Conference on Recent Trends on Electronics, Information, Communication and Technology (RTEICT)*, Aug. 2021, pp. 889–893, doi: 10.1109/RTEICT52294.2021.9573662.

[20] V. Srinadh, B. Maram, and T. Daniya, “Data security and recovery approach using elliptic curve cryptography,” 2021, doi: 10.1109/CSITSS54238.2021.9683473.

[21] S. Srinath, G. S. Nagaraja, and R. Shahabadkar, “A detailed analysis of lightweight cryptographic techniques on internet-of-things,” 2021, doi: 10.1109/CSITSS54238.2021.9683091.

[22] G. V. S. Raju and R. Akbani, “Elliptic curve cryptosystem and its applications,” *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*, vol. 2. pp. 1540–1543, 2003, doi: 10.1109/icsmc.2003.1244630.

[23] D. Mahto and D. K. Yadav, “RSA and ECC: A comparative analysis,” *International Journal of Applied Engineering Research*, vol. 12, no. 19, pp. 9053–9061, 2017.

[24] M. Q. Hong, P. Y. Wang, and W. B. Zhao, “Homomorphic Encryption Scheme Based on Elliptic Curve Cryptography for Privacy Protection of Cloud Computing,” in *Proceedings-2nd IEEE International Conference on Big Data Security on Cloud, IEEE BigDataSecurity 2016, 2nd IEEE International Conference on High Performance and Smart Computing, IEEE HPSC 2016 and IEEE International Conference on Intelligent Data and S*, 2016, pp. 152–157, doi: 10.1109/BigDataSecurity-HPSC-IDS.2016.51.

[25] S. J. Patel, A. Chouhan, and D. C. Jinwala, “Comparative evaluation of elliptic curve cryptography based homomorphic encryption schemes for a novel secure multiparty computation,” *Journal of Information Security*, vol. 5, no. 1, pp. 12–18, 2014, doi: 10.4236/jis.2014.51002.

BIOGRAPHIES OF AUTHORS

Amer Alsaraira holds a Ph.D. 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. 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. 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.

Samer Alabed is currently an associate professor, the director of accreditation and quality assurance center and the director of e-learning and academic performance improvement center at the German Jordanian University, Jordan. Further information is available on his homepage: http://drsameralabed.wixsite.com/samer. He can be contacted at email: samer.alabed@gju.edu.jo.

Omar Saraereh received the Ph.D. degree in Electrical and Electronic Engineering from Loughborough University, U.K., in 2005. 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.