Increase Security of Li-Fi Technology by Using RSA Algorithm to Encryption and Decryption Important Data

Mohammed M. Ahmed[*], Satea H. Alnajjar[**]

[*] Department of Computer Engineering, College of Engineering, Al-Iraqia University, Iraq
Email: Mohammed.m.ahmed@aliraqia.edu.iq
https://orcid.org/0009-0001-2161-169

[**] Department of Network Engineering, Al-Iraqia University, Iraq
Email: sateaahn@gmail.com
https://orcid.org/0000-0002-2828-3167

Abstract

Communication systems are constantly evolving to keep pace with the increasing number of users and their digital transactions, and the need to increase the capacity of communication networks has emerged. However, hacking and phishing operations have increased to obtain or modify users' private data. As a result, it has become necessary to enhance network security measures to protect systems and users from hacking attempts by employing encryption techniques to secure important data. In the proposed system, a communication system using advanced Li-Fi technology was developed and tested in different weather conditions and at different distances, and the system was protected using RSA technology to encrypt data and, transmit it over the network and then decrypt it at the receiving end. This approach has shown positive results with the use of large prime numbers with a high level of resistance to hacking and decryption, ensuring the secure flow of network data.

Keywords- Decryption, Encryption, FSO, Li-Fi, RSA Algorithm.

I. INTRODUCTION

The prevalence of wireless communication technologies, such as Wi-Fi, is steadily growing. Although wireless communication has achieved significant advancements, RF spectrum technology has challenges pertaining to its efficacy, capacity, availability, security, and the adverse effects of electromagnetic radiation on human health and the environment. Hence, the utilisation of the light spectrum for communication serves as a remedy for the constraints of Radio Frequency (RF) spectrum technology, with Li-Fi technology being one example. [1]. The surge in online transactions has given rise to security difficulties and vulnerabilities, including phishing, fraud, and data breaches, which erode customer trust in financial services. Security is crucial, and robust systems are needed to counter these threats. It has become necessary to develop solutions that focus on the security and integrity of transactions while maintaining user comfort[2]. Safeguarding information is a crucial concern when it comes to delivering messages and data in the modern era of technology. However, due to the increasing complexity of cyber threats, it is necessary to implement a robust plan to protect the security and reliability of data transmitted over the internet[3]. FSO communication systems, one of the most popular wireless communication technologies, have grown in popularity and development over the past decade. FSO can fulfil the rapidly expanding bandwidth need as a novel alternative to the present technology. Most notably, FSO systems may substitute optical fibre cable when it cannot be deployed or is expensive [4]. Optical wireless communication refers to data transmission using light waves instead of traditional wired or radio frequency methods. White LEDs may be used for illumination and data transmission in several upcoming applications, indoors or outdoors. This has the capacity to result in significant energy preservation on a worldwide level. As a result, there is an increasing need for telecommunications services that can accommodate a broad range of frequencies, high data rates, and excellent service quality [5] [6]. VLC technology emerged as a new communication technology alternative due to its broad unlicensed spectrum, ease of availability, extended lifespan, compact size, and low power consumption. Additionally, Due to its immunity to radio-frequency interference, this device is well-suited for internal communication purposes [7].

Text encryption is a method employed to protect the secrecy of information in digital communications[8]. The RSA encryption method was developed by three academics from MIT, namely Ron Rivest, Adi Shamir, and Len Adleman. Their work was presented in a 1978 essay titled "A Method for Obtaining Digital Signatures and Cryptosystems of the Public Key."[9]. The primary purpose of the RSA algorithm is to guarantee the integrity, secrecy, authenticity, and nonrepudiation of data. Additionally, RSA offers enhanced capabilities for key exchange and digital signatures. RSA involves the use of public and private keys to perform encryption and decryption. The procedure entails the production of keys, whereby both the public and private keys are produced[10]. The primary motivation for utilising the RSA technique is the inherent difficulty in factoring big numbers. The security is achieved by utilising the product of two big prime integers throughout the implementation of the method. The most intricate aspect of RSA cryptography is in the process of generating the public key and private key [11].

One of the challenges facing Li-Fi technology, like other technologies, the security is directly correlated with the rise in the number of users and integrity of data and preventing hackers from accessing it. The main goal is to achieve Li-Fi with good performance and security that provides users with an efficient, fast and secure service. The goal of writing this research is to encrypt important data before sending it using MATLAB to prevent hackers from violating users' privacy and exploiting or manipulating their data. The encryption is then decrypted and the data is returned to its original format at the receiving end, which provides a secure and reliable service for network users. The rest of the paper is arranged in this way. This paper consists of five parts: The study specifics are presented in the second section, the RSA method is explained in the third section, the results are outlined in the fourth section, and the conclusions are provided in the fifth section.

II. RESEARCH ELABORATIONS

The proposed system is configured using Opti system V17 FSO channel, supporting 10 Gbps data rate. The design consists of a VLS system connected to a room with six end users, as shown in Figure 1.

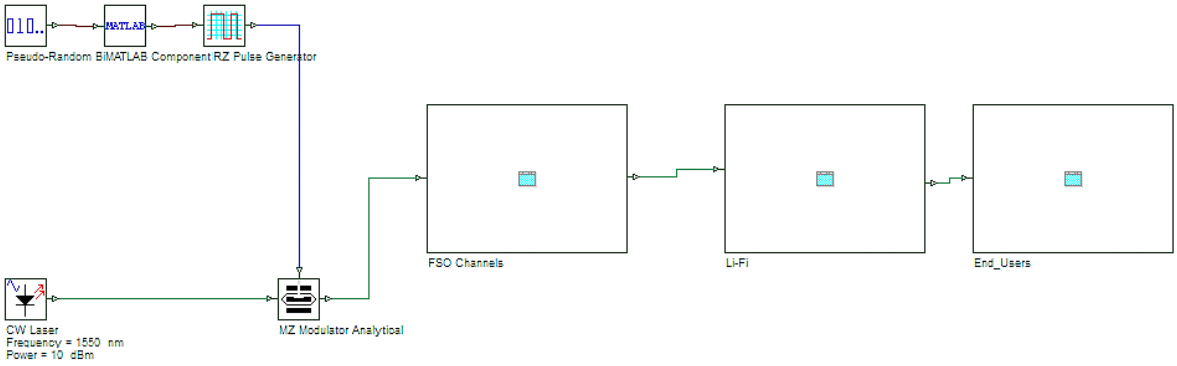

Figure 1. Proposed system design

A. *Transmitter Module*

The four components of the transmitter. To produce a 10 Gbps NRZ signal, there is an NRZ transmitter. The output of the MATLAB bit sequence generator is placed in a pulse generator. An externally modulated laser operating at a wavelength of 1550 nm is modulated using NRZ pulses. The Mach-Zehnder modulator is an interferometric intensity modulation device. It implements a continuous wave (CW) laser. The output is sent to the FSO channel as shown in Figure 2.

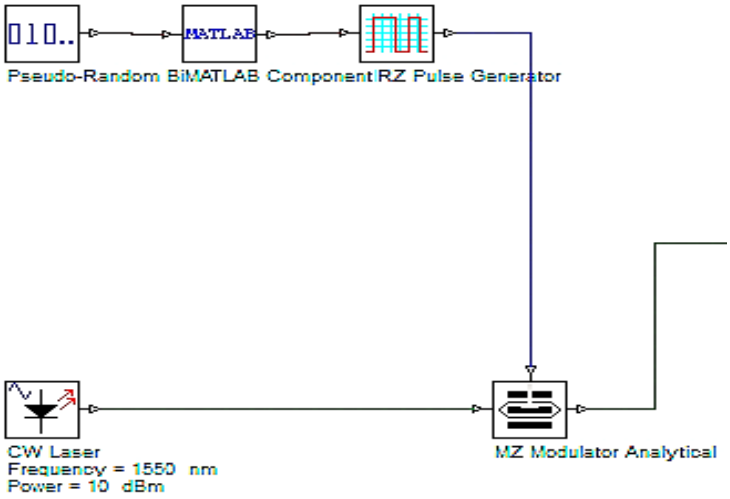

Figure 2. Transmitter part design

B. *free space optic*

A Free-Space Optical (FSO) communication system transmits optical information wirelessly over air [12]. FSO is a line-of-sight point-to-point method that needs clarity between transmitter and recipient. Once modulated, the infrared or visible beam is

delivered over the air [13]. Consequently, it is more appropriate for situations in which the physical link is down and a significant amount of data must be transferred[14]. See Fig 3. FSO design features are listed in Table (1).

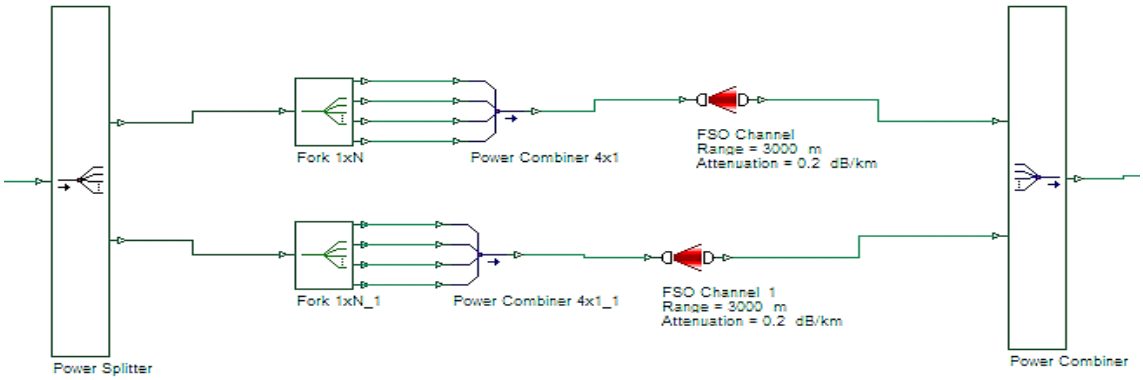

Figure 3. The FSO channel part design

TABLE I. THE FSO ELEMENTS

Element	value
Range	100_200 m, 1_2.5 Km
Attenuation	10 dB, 242 dB
Aperture's Diameter of the receiver	25 cm
Aperture's Diameter of the transmitter	2.5cm
Beam divergence	1mred

C. *Light Fidelity*

Li-Fi, an advanced optical wireless communication technology, holds significant potential compared to other solutions due to the energy and cost efficiency of the light-emitting diode (LED) [15]. Li-Fi may fulfil this requirement by using its numerous benefits, such as achieving high data transfer speeds, minimising electromagnetic interference, and providing indoor localisation capabilities. [16][17]. s shown in Figure 4.

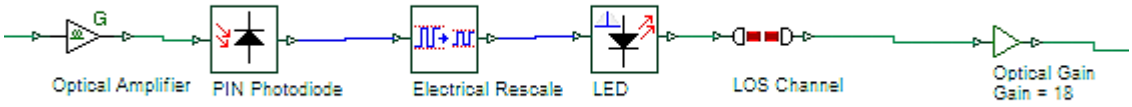

Figure 4. The Li-Fi channel part design

- Light-Emitting Diodes (LEDs)
- The LED functions as the transmitter. Initially, the electrical signal is transformed into the appropriate voltage to directly provide power to the LED source, subsequently regulating the lights' luminosity [7]. Table (2): LED components.

TABLE II. ELEMENTS OF LED

Element	Value
Quantum efficiency	0.65
Electron Carrier Lifetime	1×10^{-12} s
Frequency	550nm
RC Time Constant	1×10^{-12} s

The optical power of the LEDs is provided by [18]is as follows:

$$p = \eta . h . f \frac{i(t)}{q} \qquad (1)$$

The notions of "quantum efficiency" (h), "emission frequency" (f), "electron charge" (q), and "modulation current signal" (i(t)) are all interrelated through their dependence on Planck's constant.

- line-of-sight

AS illustrated in Figure 4, The LED sends the modulated signal to the receiver (PD) via LOS. Table (3) lists simulator defaults.

TABLE III. THE ELEMENTS OF LINE OF SITE CHANNEL

Element	Value
Transmitter Half - Angle	60deg
Irradiance Half - Angle	20deg
Range	3m
Incidence	20 deg

The pattern is as follows when the emission density has a Lambertian[19]:

$$R_{\emptyset} = \begin{Bmatrix} \frac{m+1}{2\pi} \text{Cos}^{\,m}\, \emptyset, \text{For } \emptyset \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right] \\ 0, \text{Otherwise} \end{Bmatrix} \qquad (2)$$

The transmitter's Semi-Angle is $\boldsymbol{\phi}1/2$ as, where ϕ is the radiation angle and m is the Lambertian order.

$$m = \frac{-\log 2}{\log[\cos(TransmitterHalfAngle)]} \qquad (3)$$

- Amplifiers

  It is a device that operates directly with optical signals. The optical amplifier utilises stimulated emissions to amplify optical signals. The processing is achieved by interacting the primary photon of the amplifier with an excited electron at a specified frequency, resulting in a reduction of the energy level [20].

  There is no need for the use of repeaters. The Optical amplifiers increase the network because their characteristics, such as reduced losses, are more stable and efficient across long distances [21]. It compensates for fiber loss, low signal, and connection loss while transmitting long distances [22]. It's also used to increase photodetector sensitivity and in the transmitter's last step. [23].

D. Receiver Design

The receiver design comprises six users, as depicted in Figure 5, of a demultiplexer. The demultiplexer's output is then transmitted to a PIN photodetector, which converts the optical signals into electrical signals. The signal is subsequently transmitted through a low-pass filter with a bandwidth of 0.75 Hz, namely an LPGF (low-pass Gaussian filter). Following that is a 3R generator that restores the electrical signal. This generator relies on an NRZ pulse generator and a data recovery component. It produces both the original bit sequence and a modified electrical signal for study of Bit Error Rate (BER). The eye diagram is produced utilising the output of the bit error rate (BER) analyser, which also provides information on the system's BER performance and quality factor. MATLAB is utilised to execute the algorithm on the encrypted data that has been received, in order to decipher it and present it to the consumers in its original format.

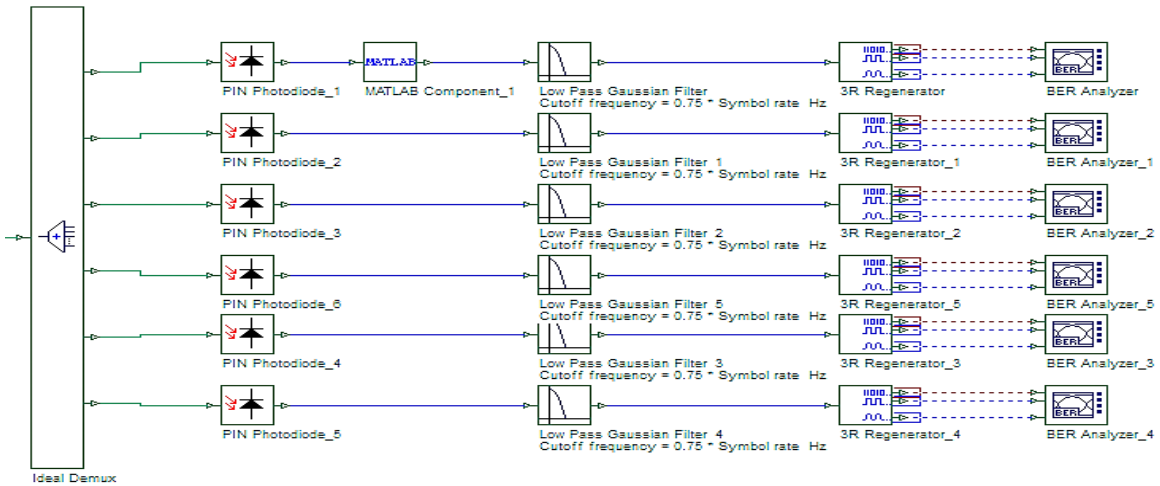

Figure 5. Receiver Side Design

III. RSA ALGORITHM

Cryptography is a mathematical engineering field that secures data, secrecy, and authentication [24]. Decryption cleans up communications while encryption scrambles them [25]. Cryptography may be classified into two main categories: symmetric and asymmetric. Both the encryption and decryption methods utilise symmetric keys. The public and private keys make up the asymmetric key. Decryption uses the private key, whereas encryption uses the public key[26].
Common asymmetric methods include the RSA algorithm. Keys are made by multiplying two large prime integers. Decoding uses the secret key, Whereas encryption uses the public key[27]. The security of the RSA method is based on the challenging task of factoring huge prime integers. The process of factoring is performed in order to get the private key [28].

- Steps of RSA Algorithm
  See Figure 6 for more information. Initial step: Pick two prime numbers, p and q. The next thing we need to do is find n, which is the modulus for both the public and private keys. The key length, which is usually given in bits, is a way to measure how big it is. We need to figure out Euler's totient ϕ (n). ϕ is Euler's totient function in this case. This rate is not shared. The next step is to choose a number e such that e < ϕ (n) and gcd (e, ϕ (n)) = 1. Next, we can use the equation d ≡ e − 1 (mod ϕ(n)) to find d's value. Here, d is the modular inverse of e modulo ϕ(n). The operation is carried out by finding d, which is shown by d · e ≡ 1 (mod ϕ (n)). We use the expanded Euclidean method to figure this out. People use the fake code from the section on modular numbers, where a and n stand for e and ϕ, respectively. Discover the secret key d.

```
% RSA Encryption and Decryption for Text Messages
% Step 1: Generate two large prime numbers, p and q
p = 11939;
q = 193939;

% Step 2: Compute n = p*q
n = p*q;

% Step 3: Compute Euler's totient function, phi(n)=(p-1)*(q-1)
phi_n = (p-1)*(q-1);

% Step 4: Choose public key exponent, e such that 1 < e < phi(n) and gcd(e, phi(n)) = 1
e = 1073676287;

% Step 5: Compute private key exponent, d such that d*e ≡ 1 (mod phi(n))
d = modInverse(e, phi_n);
```

Figure 6. The steps of RSA algorithm

- The values of n and e are used in the public key. The number of the private key is n and d, and it is kept hidden. The numbers of p, q, and ϕ(n) are kept secret because they can be used to figure out d.

- Encryption
  The sender encrypts message m using receiver's public key (e, n):
  The congruence c ≡ me (mod n) is true when, In this context, the variables c, m, e, and d represent the encrypted text, plain text, public key, and private key, respectively.

- Decryption
  The recipient decrypts the cipher text c using their private key (d, n) by using the equation m ≡ cn (mod n), where c represents the cipher text, m represents the plain text, e represents the public key, and d represents the private key.
  Decryption of communications encrypted with the matching public key is only possible for the specified private key holder. Asymmetric encryption and decryption, which relies on mathematically linked key pairs, avoids the requirement of discreetly exchanging a common key, as is essential with symmetric ciphers.

IV. RESULT AND DISCUSSION

Results of proposed system design Effective Weather Condition, the system was tested for the BER, Q-factor and eye diagram are included in the findings; in addition, In the rainy weather and different distances with BER as shown in Figure (7A) and Q-Factor as shown in Figure (7B) that rain conditions were used with more than one range. The results were very satisfactory, where the eye diagram was taken at 1km. as shown below in Figure (7C).

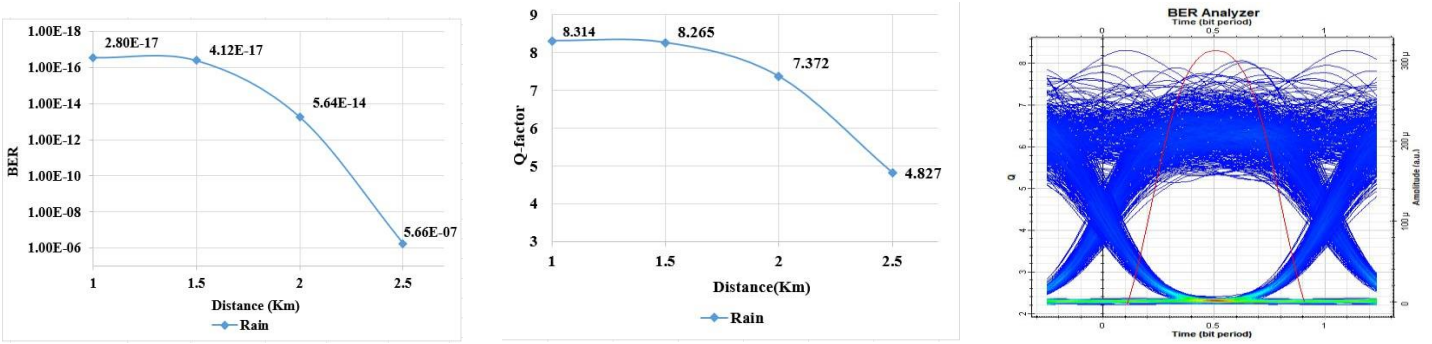

Figure 7. The rain weather with (A)BER. (B) Q-Factor. (C) eye diagram

Furthermore, in heavy dust weather, Figure (8A) Shows BER in the different distances, and Q-Factor as shown in Figure (8B) that rain conditions were used with more than one range. The results were very satisfactory, where the eye diagram was taken at 100m. as shown below in Figure (8C).

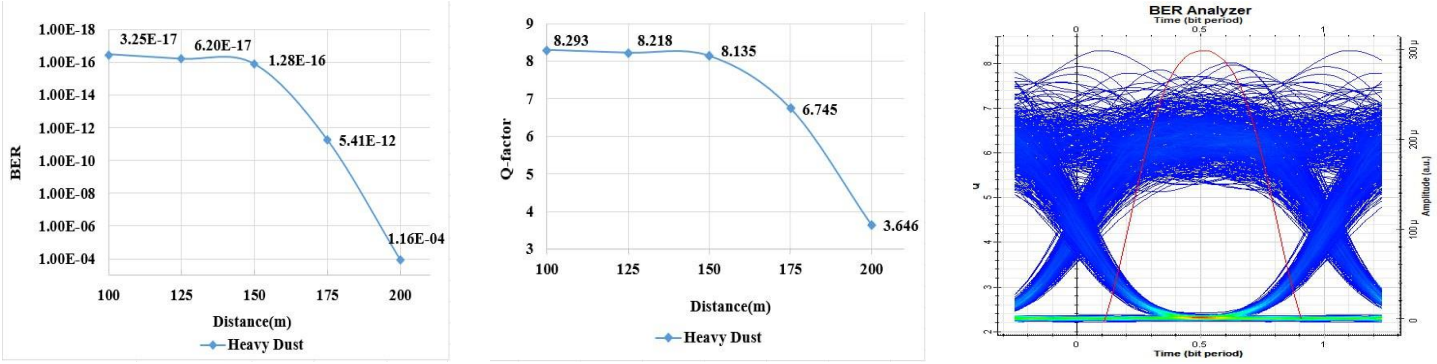

Figure 8. The heavy dust weather with (A)BER. (B) Q-Factor. (C) eye diagram

The RSA algorithm employs the discrete logarithm method for its implementation. In our study effort, we have utilised the RSA method to ensure the security of text. Due to its utilisation of the discrete logarithm method, the RSA algorithm has been widely employed in various real-world applications to ensure information security. Therefore, we have chosen to utilise this technique for information security purposes, as seen in Figure 9.

Figure9. MATLAB workspace for RSA encryption and decryption

Figure 10 shows how a secret key encrypts email information. The receiver receives consecutive bits via FSO channel. The recipient decrypts the encrypted text using their private key. Better information security is achieved with the suggested encryption method.

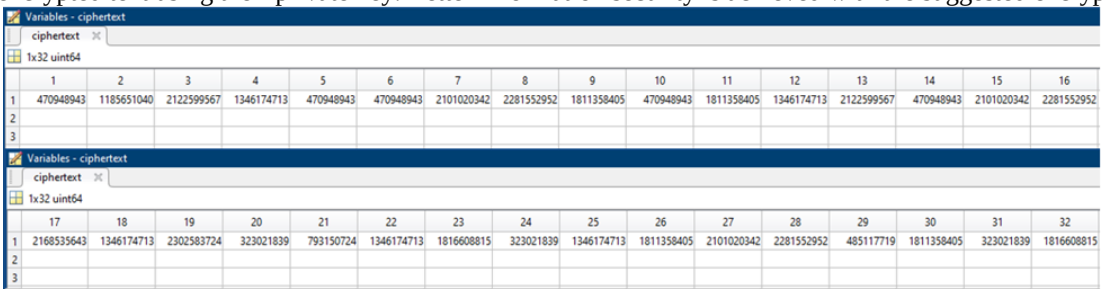

Figure 10. The cipher text for 32 characters

In decryption, the resulting cipher text is decrypted using the RSA algorithm. The resulting decrypted text is shown in Figure 11 and is the same as the original text.

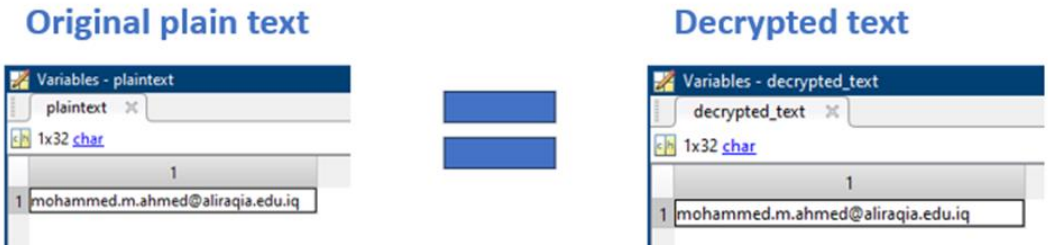

Figure 11. The decrypted text with original text

V. CONCLUSION

This research tested the Li-Fi system in different weather conditions and at different distances. It achieved good results in transferring encrypted data over the network in a secure manner, as it achieved BER results from 3.25 * 10-17 to 5.41 * 10-12 and the Q factor ranged from 8.314 to 6.745. The efficiency of the RSA algorithm was also proven in successfully encrypting data and retrieving it to the end user in its original form without any change or loss. The proposed system has proven its ability to improve the performance of Li-Fi technology in terms of security, which makes the network safe for users to maintain privacy and save data from hackers. If hackers can penetrate the network, they will not be able to read the data because it is sent over the network using a high-level code that is difficult to decode without the private key.

REFERENCES

[1] Darussalam and G. Arief, "Jurnal Resti," *Resti*, vol. 1, no. 1, pp. 19–25, 2018.
[2] N. J. Hamad, A. A. Abdulhameed, and M. H. Ali, "Enhancing Security and Efficiency through QR Integration with Hybrid AES-ECC Algorithm in Mobile Apps for Cardless Data Transactions," *Al-Iraqia J. Sci. Eng. Res.*, vol. 2, no. 4, 2023, doi: 10.58564/ijser.2.4.2023.124.
[3] Y. Ramadhan, S. Suhardi, and Y. Aditama, "Data security using low bit encoding algorithm and rsa algorithm," *J. Mantik*, vol. 8,no.1,2024,[Online].Available:http://iocscience.org/ejournal/index.php/mantik/article/view/4945%0Ahttps://iocscience.org/ejournal/index.php/mantik/article/download/4945/3471.
[4] S. A. Al-Gailani *et al.*, "A Survey of Free Space Optics (FSO) Communication Systems, Links, and Networks," *IEEE Access*, vol. 9, pp. 7353–7373, 2021, doi: 10.1109/ACCESS.2020.3048049.
[5] S. H. Alnajjar and B. K. Alfaris, "Enhancement of Light Fidelity System According to Multi-Users Utilizing OCDMA Technology under Weather Conditions," *Al-Iraqia J. Sci. Eng. Res.*, vol. 1, no. 2, pp. 9–15, 2023, doi: 10.33193/ijser.2.1.2022.47.
[6] N. T. Almalah, "Evaluating Li - Fi System Performance in the Presence of External While Light Interference," vol. 3, no. 3, 2024.
[7] S. H. Alnajjar and B. K. Alfaris, "OCDMA Performance on FSO Turbulent Weather Channel on Li-Fi Systems," *Al-Iraqia J.*

Sci. Eng. Res., vol. 1, no. 2, pp. 1–7, 2023, doi: 10.33193/ijser.2.1.2022.46.

[8] S. Arifin, D. Wijonarko, Suwarno, and E. K. Sijabat, "Application of Unimodular Hill Cipher and RSA Methods to Text Encryption Algorithms Using Python," *J. Comput. Sci.*, vol. 20, no. 5, pp. 548–563, 2024, doi: 10.3844/jcssp.2024.548.563.

[9] F. H. M. S. Al-Kadei, H. A. Mardan, and N. A. Minas, "Speed Up Image Encryption by Using RSA Algorithm," *2020 6th Int. Conf. Adv. Comput. Commun. Syst. ICACCS 2020*, no. March, pp. 1302–1307, 2020, doi: 10.1109/ICACCS48705.2020.9074430.

[10] A. Yeboah-Ofori and A. Ganiyu, "Big Data Security Using RSA Algorithms in A VPN Domain," *Int. Conf. Artif. Intell. Comput. Data Sci. Appl. ACDSA 2024*, 2024, doi: 10.1109/ACDSA59508.2024.10467364.

[11] A. Sahoo, P. Mohanty, and P. C. Sethi, "Image Encryption Using RSA Algorithm," *Lect. Notes Networks Syst.*, vol. 431, no. May, pp. 641–652, 2022, doi: 10.1007/978-981-19-0901-6_56.

[12] E. Jarangal and D. Dhawan, "Comparison of channel models based on Atmospheric turbulences of FSO system-A Review," *Int. J. Res. Electron. Comput. Eng.*, vol. 6, no. 1, pp. 282–286, 2018.

[13] S. H. Alnajjar and A. Majid Hameed, "Effect of Bidirectional Reflector Technology on the Non-line-of-sight propagation of Light Fidelity System," in *2021 3rd International Conference on Electronics Representation and Algorithm (ICERA)*, IEEE, Jul. 2021, pp. 29–34. doi: 10.1109/ICERA53111.2021.9538644.

[14] R. Gupta and P. Singh, "Hybrid FSO-RF system: a solution to atmospheric turbulences in long haul communication," *Int. J. Sci. Eng. Res.*, vol. 5, no. 11, pp. 602–605, 2014.

[15] M. G. Al-Hamiri and H. J. Abd, "Designing a LiFi Transceiver based Space Time Block Coding with different pulses," in *2022 3rd Information Technology To Enhance e-learning and Other Application (IT-ELA)*, IEEE, Dec. 2022, pp. 110–115. doi: 10.1109/IT-ELA57378.2022.10107931.

[16] M. G. Al-Hamiri and H. J. Abd, "Design and performance evaluation of a hybrid LiFi transceiver using OSTBC-based spatial multiplexing and transmit diversity," *e-Prime - Adv. Electr. Eng. Electron. Energy*, vol. 6, p. 100283, Dec. 2023, doi: 10.1016/j.prime.2023.100283.

[17] N. T. Almalah, F. E. Mahmood, and M. T. Yassen, "Li - Fi Technology in Optical Communication Systems : A Review," vol. 3, no. 3, pp. 163–171, 2024.

[18] "No Title", doi: "Optiwave Systems, https://optiwave.com." (accessed.

[19] J. R. Barry, J. M. Kahn, W. J. Krause, E. A. Lee, and D. G. Messerschmitt, "Simulation of Multipath Impulse Response for Indoor Wireless Optical Channels," *IEEE J. Sel. Areas Commun.*, vol. 11, no. 3, pp. 367–379, 1993, doi: 10.1109/49.219552.

[20] S. Lertampaiporn, T. Vorapreeda, A. Hongsthong, and C. Thammarongtham, "Ensemble-AMPPred: Robust AMP Prediction and Recognition Using the Ensemble Learning Method with a New Hybrid Feature for Differentiating AMPs," *Genes (Basel).*, vol. 12, no. 2, p. 137, Jan. 2021, doi: 10.3390/genes12020137.

[21] D. Malik, K. Pahwa, and A. Wason, "Performance optimisation of SOA, EDFA, Raman and hybrid optical amplifiers in WDM network with reduced channel spacing of 50 GHz," *Optik (Stuttg).*, vol. 127, no. 23, pp. 11131–11137, Dec. 2016, doi: 10.1016/j.ijleo.2016.09.047.

[22] A. Hassan, A. Aboshosha, and M. El_Mashade, "Analysis of Gain and NF using Raman and hybrid RFA-EDFA," *J. Multidiscip. Eng. Sci. Technol.*, vol. 4, no. 10, pp. 8482–8487, 2017.

[23] S. FE and K. MS, "Comparison of EDFA and Raman amplifiers effects on RZ and NRZ encoding techniques in DWDM optical network with bit rate of 80 Gb/s," *Phys. Astron. Int. J.*, vol. 2, no. 1, pp. 116–121, 2018, doi: 10.15406/paij.2018.02.00057.

[24] B. Purnama and A. H. H. Rohayani, "A New Modified Caesar Cipher Cryptography Method with LegibleCiphertext From a Message to Be Encrypted," *Procedia Comput. Sci.*, vol. 59, pp. 195–204, 2015, doi: 10.1016/j.procs.2015.07.552.

[25] Rismayani and C. Susanto, "Using AES and DES Cryptography for System Development File Submission Security Mobile-Based," in *2020 8th International Conference on Cyber and IT Service Management (CITSM)*, IEEE, Oct. 2020, pp. 1–7. doi: 10.1109/CITSM50537.2020.9268805.

[26] C. B, K. K. V, and S. R. C, "A Survey on Various Lightweight Cryptographic Algorithms on FPGA," *IOSR J. Electron. Commun. Eng.*, vol. 12, no. 01, pp. 54–59, 2017, doi: 10.9790/2834-1201025459.

[27] R. Apau and C. Adomako, "Design of Image Steganography based on RSA Algorithm and LSB Insertion for Android Smartphones," *Int. J. Comput. Appl.*, vol. 164, no. 1, pp. 13–22, 2017, doi: 10.5120/ijca2017913557.

[28] Jamaludin and Romindo, "Implementation of Combination Vigenere Cipher and RSA in Hybrid Cryptosystem for Text Security," *Int. J. Inf. Syst. Technol. Akreditasi*, vol. 4, no. 1, pp. 471–481, 2020.