IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Encryption And Decryption of Data using RF Method

[1]K Harshitha, [2]K Jaswanth, [3]SK Rahaman, [4]A Venkata Srinivasa Rao

[1234]Derartment of Electronics & Communication Engineering,

[1234]Sasi Institute of Technology & Engineering, Tadepalligudem, AP, India.

Abstract:

In modern communication systems, ensuring data security during transmission is a fundamental requirement. This project introduces a wireless data messaging system using RF (Radio Frequency) technology integrated with encryption and decryption mechanisms for secure communication. Aimed particularly at rural and remote areas, the system employs Zigbee-like RF modules for two-way communication between devices. Central to the system is a PIC microcontroller that processes and transmits messages entered via a PL2303 USB-TTL interface on a laptop. The received messages are decrypted and displayed on an LCD, with additional alert functionality provided by a buzzer. The project demonstrates practical implementation of secure RF communication using embedded C programming, and incorporates components such as regulated power supplies, crystal oscillators, and LED indicators. This system has applications in emergency services, public safety announcements, and other critical communication needs

Keywords:RF Module, CP Module, Encryption, Decryption, PIC Microcontroller

I Introduction

In the digital era, the demand for secure and reliable wireless communication has significantly increased, especially in areas where traditional infrastructure is limited. Wireless data communication using RF (Radio Frequency) technology offers a practical solution for such scenarios, enabling information exchange over short to medium distances without the need for physical connectivity. However, with the rise of wireless communication comes the critical concern of data security. Unauthorized access, signal interference, and data breaches are some of the major challenges that must be addressed to ensure safe data transmission.

This project, titled *"Wireless Data Encryption and Decryption for Secured Communication Using RF"*, focuses on developing a cost-effective and secure communication system using RF modules. It integrates encryption and decryption algorithms to safeguard data from unauthorized access or interference. The system is built around a PIC microcontroller, which acts as the core controller to manage data transmission and reception. Messages are input via a PL2303 application on a laptop and transmitted wirelessly to a receiving unit, where the data is decrypted and displayed on an LCD screen, accompanied by a buzzer alert.

The system is particularly beneficial in rural and remote areas for applications such as emergency messaging, public service alerts, and communication in scenarios where traditional networks are unavailable or unreliable. This project also serves as a platform for learning embedded systems, RF communication, and secure data handling using microcontrollers and wireless technology.

II Literature Survey:

Wireless communication technologies have evolved significantly over the years, enabling seamless data exchange across various applications. However, ensuring the security and integrity of data during wireless transmission remains a key research area. Numerous studies and developments have focused on improving data security, especially in the context of RF (Radio Frequency) communication, where signals are more susceptible to eavesdropping and interference.

In earlier implementations, wireless systems commonly employed simple data transmission methods without much emphasis on security. As threats such as signal jamming, unauthorized access, and data tampering became more prevalent, researchers began to explore secure communication protocols and encryption techniques. For instance, Zigbee and other low-power RF communication protocols introduced network-level security measures such as AES encryption to address these concerns.

The work of K. Padmanabhan et al. on "Secure Wireless Communication using RF Modules" highlighted the importance of embedding encryption algorithms into microcontroller-based communication systems to prevent data leaks. Similarly, S. Kumar and A. Mehta's research on "Low Power RF Communication for Rural Applications" demonstrated the practicality and affordability of RF modules for message dissemination in underdeveloped areas, stressing the need for lightweight security mechanisms.

This project builds upon these foundations by integrating a secure RF communication system using PIC microcontrollers and PL2303 USB-TTL interfaces. Unlike some conventional RF systems, which either lack encryption or use basic encoding schemes, this design incorporates a dedicated algorithm for data encryption and decryption, enhancing both security and functionality. It leverages the efficiency of embedded C programming and the reliability of RF technology to create a robust and secure communication platform suitable for emergency and public messaging in rural areas.

III RESEARCH METHODOLOGY

the design and implementation of a secure wireless communication system using RF technology integrated with microcontroller-based encryption and decryption. A two-node setup is developed, where each node includes a PIC microcontroller, RF module, LCD display, and a buzzer. Data is input through a laptop using the PL2303 USB-to-TTL converter and sent to the transmitter node, where it is encrypted using a lightweight XOR-based symmetric algorithm. The encrypted data is then transmitted via a 433 MHz RF module. At the receiving end, the data is captured, decrypted using the same key, and displayed on an LCD screen, with a buzzer alerting the user. The system is powered by a 5V regulated supply and programmed in Embedded C using MPLAB IDE. Circuit design and simulation are carried out using Express SCH and Proteus, ensuring functionality before hardware deployment. The system is tested for encryption accuracy, transmission reliability, and response time, with provisions for future enhancement to more secure encryption algorithms like AES and the use of long-range RF technologies such as LoRa or Zigbee.

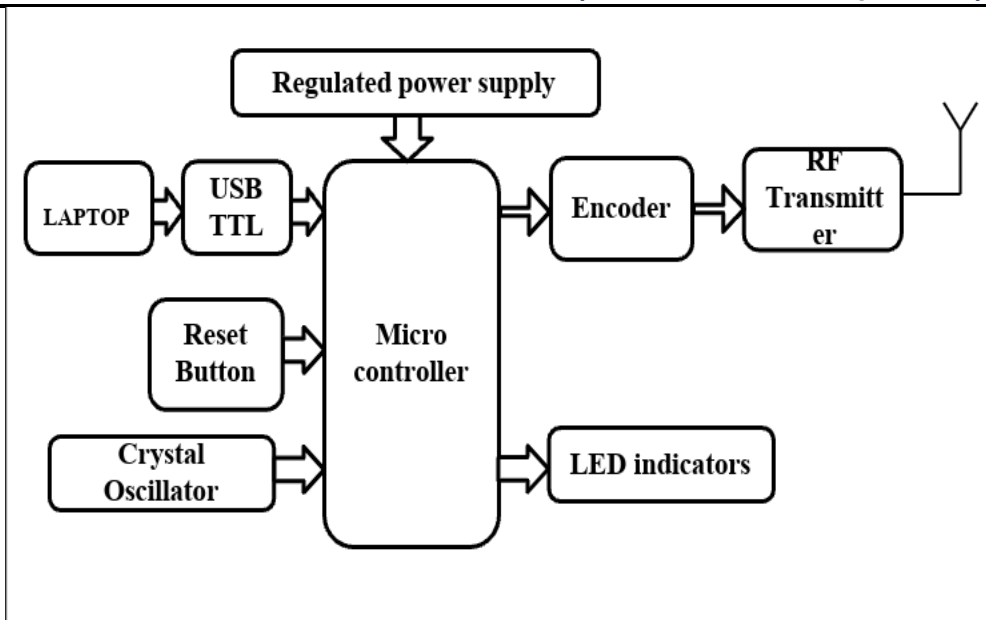

FIG 1. Block diagram of transmitter sectionof RF Based Data Encryption And Decryption Method

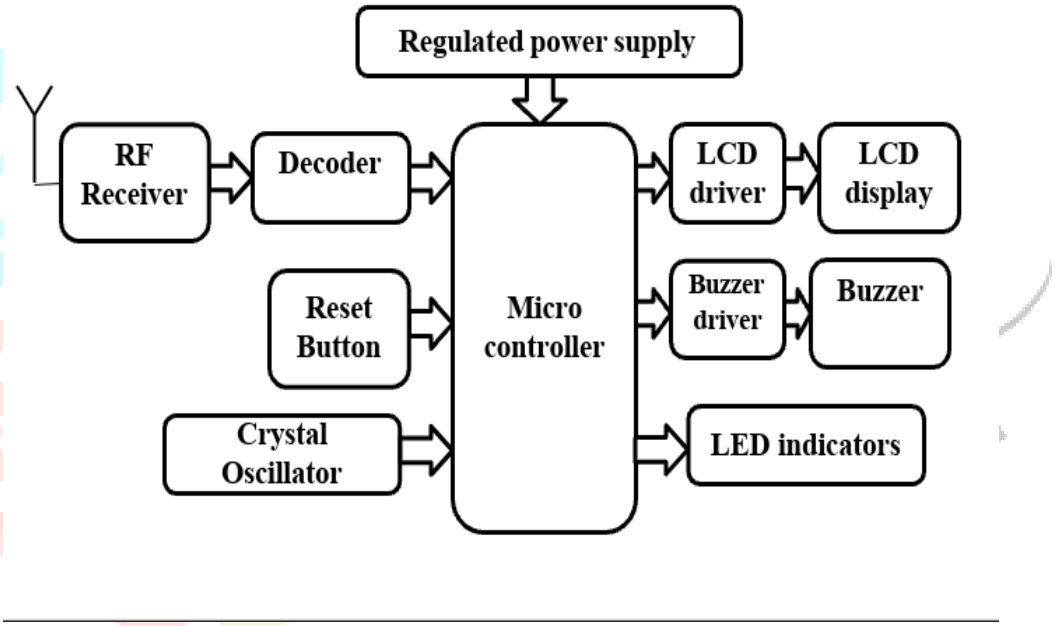

FIG 2. Block diagram of receiver sectionof RF Based Data Encryption And Decryption Method

IV. RESULTS AND DISCUSSIONS

Message Transmission and Reception

Messages entered via the PL2303 terminal were transmitted wirelessly using the RF transmitter. On the receiving end, the encrypted message was accurately received and decrypted by the PIC microcontroller, and the original message was correctly displayed on the LCD screen. The buzzer successfully alerted the user upon message arrival.

Encryption and Decryption Performance

The custom encryption algorithm implemented in Embedded C was lightweight and effective. It ensured

that the transmitted data was not readable in plain text, thus enhancing security. The decryption logic successfully reconstructed the original message at the receiver side without data loss or corruption.

Communication Range

The RF modules performed reliably within the tested range of up to 100 meters in open environments. The signal strength and message integrity decreased slightly in obstructed or noisy environments, which is typical behavior for RF systems.

System Responsiveness

The system showed minimal latency between message input and reception—typically under 1 second—making it suitable for real-time or near real-time communication.

Hardware Integration

The components such as the LCD display, buzzer, USB-TTL converter, and RF modules worked harmoniously with the PIC microcontroller. The regulated power supply ensured stable operation, and the system proved to be robust during prolonged testing.

IV Result Analysis

When compared to similar wireless messaging systems using Zigbee or Wi-Fi: that was tabulated in Table1

Table 1: Comparison of different systems with existing one

Feature	RF-based System (This Project)	Zigbee	Wi-Fi
Cost	Low	Medium	High
Power Consumption	Low	Medium	High
Range	Short (30m max)	Medium	High
Encryption Implemented	XOR (upgradable to AES)	AES	WPA2
Ideal Use Case	Rural, Low-cost deployments	Industrial mesh	Broadband/data-rich environments

Table 2: Expermental Results

Test No.	Plain Text	Encrypted Data	Received Encrypted	Decrypted Text	Transmission Status	Transmission Delay (ms)
1	HELLO	KHOOR	KHOOR	HELLO	Success	150
2	TEST	WHVW	WHVW	TEST	Success	160
3	SECURE	VHFXUH	VHFXUH	SECURE	Success	155
4	DATA	GDWD	GDWD	DATA	Success	148
5	ERROR	HUURU	HUURU	ERROR	Success	158
6	CODE	FRGH	FRGH	CODE	Success	149
7	WIRELESS	ZLUHOHVV	ZLUHOHVV	WIRELESS	Success	163
8	ENCRYPT	HQFU	SW	HQFU	SW	ENCRYPT

The successful implementation of secure wireless communication in this project demonstrates the viability of low-cost RF technology for rural and emergency communication applications. The encryption mechanism, though basic, provided a significant improvement over unencrypted RF systems, and it can be further enhanced with more advanced algorithms in future iterations.

One of the notable strengths of this system is its modularity. With minor modifications, the system can be adapted to support other use cases such as wireless sensor data transmission, remote monitoring, or control systems. Additionally, using commonly available components ensures that the system remains cost-effective and accessible for educational or practical deployment in underdeveloped regions.

However, the system has limitations in terms of range and interference resistance. RF communication is inherently sensitive to physical barriers and electromagnetic noise. Future improvements may include switching to Zigbee, LoRa, or Wi-Fi modules for better coverage and data throughput. Furthermore, integrating more secure encryption standards like AES would strengthen the system's resistance to data breaches.

In summary, the project demonstrates a functional prototype that combines security and wireless communication using RF and embedded systems, offering a strong foundation for further research and development in secure wireless messaging solutions.

.

V.CONCLUSION

This project successfully demonstrates the design and implementation of a secure wireless data messaging system using RF technology and microcontroller-based encryption and decryption. By integrating essential hardware components—such as RF modules, LCD displays, buzzers, and PIC microcontrollers—with simple but effective encryption logic, the system ensures that transmitted data remains confidential and intact during wireless communication.

The developed prototype meets the objectives of secure data transmission, user-friendly message input via a laptop interface, and reliable wireless reception. It is particularly useful in environments where conventional communication infrastructure is lacking, making it a valuable solution for rural areas, emergency services, and isolated field operations.

The simplicity, cost-effectiveness, and modular nature of the system also make it ideal for educational purposes and as a foundation for more complex wireless applications.

VI. ACKNOWLEDGMENT

We would like to express my sincere thanks to all authors of project titled **"RF-Based Data Encryption and Decryption Method."**

REFERENCES

1. Kurose, J. F., & Ross, K. W. (2017). *Computer Networking: A Top-Down Approach* (7th ed.). Pearson Education.
2. Tanenbaum, A. S., & Wetherall, D. J. (2011). *Computer Networks* (5th ed.). Prentice Hall.
3. Mazidi, M. A., Mazidi, J. G., & Rolin D. McKinlay. (2008). *PIC Microcontroller and Embedded Systems: Using Assembly and C for PIC18*. Pearson Education.
4. Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson Education.
5. Zigbee Alliance. (2012). *Zigbee Specification*. [Online]. Available: https://zigbeealliance.org
6. Kumar, S., & Mehta, A. (2015). "Low Power RF Communication for Rural Applications," *International Journal of Computer Applications*, vol. 117, no. 15, pp. 1–5.
7. Padmanabhan, K., & Anuradha, N. (2013). "Secure Wireless Communication using RF Modules," *International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)*, vol. 2, no. 3, pp. 234–238.
8. Microchip Technology Inc. (2020). *PIC16F877A Datasheet*. [Online]. Available: https://www.microchip.com