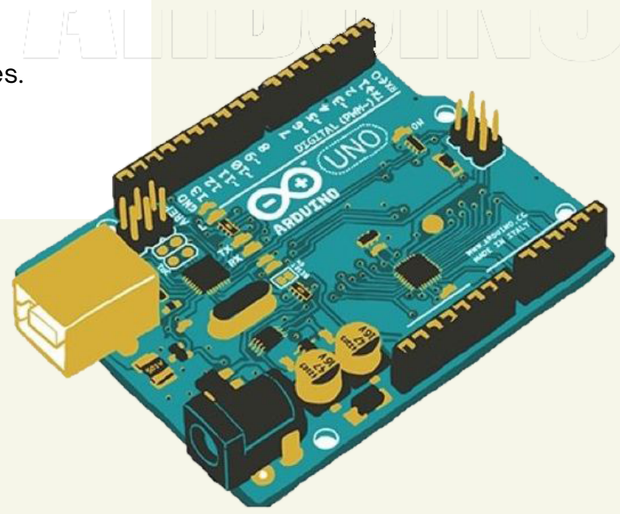
SENDING ENCRYPTED MESSAGE USING ARDUINO

Our project aims to develop a robust message communication system utilizing Arduino Uno and NRF24 modules. The system will focus on ensuring secure data transmission by incorporating RSA encryption and decryption algorithms.



GALALA UNIVERSITY
Powered by Arizona State University

Students
Youssef Mohamed Ahmed, 221101573
Mahitab Waleed Mohamed, 221100429
Youssef Mohamed Reda, 221101020
Youssef Yehia Abosrewa, 221101030

Supervisor
Dr. Mohamed Abdelaziz

Subject
Discrete Mathematics (CSE 315)

Introduction

In today's interconnected world, the ability to exchange messages securely and efficiently has become increasingly important. In this context, Arduino Uno, a popular microcontroller board, combined with the NRF24 wireless communication module, offers a versatile platform for sending and receiving messages wirelessly. To enhance the security of these messages, the implementation of the RSA encryption algorithm provides a robust and reliable solution.
The Arduino Uno, with its compact size and low power consumption, serves as an ideal choice for building small-scale communication systems. When paired with the NRF24 module, it allows for reliable long-range communication over the 2.4GHz frequency band. This combination enables seamless wireless data transmission between devices.
RSA (Rivest-Shamir-Adleman) is a widely-used asymmetric cryptographic algorithm that relies on the mathematical properties of large prime numbers. It involves generating a pair of keys: a public key for encrypting the message and a private key for decrypting it. The public key can be freely shared with anyone, while the private key must be kept confidential by the receiver.

Objective

The primary objectives of this project are as follows:

- Establishing Wireless Communication: Set up a reliable wireless communication channel using the NRF24 modules
- Implementing RSA Encryption: Integrate the RSA encryption algorithm into the system to provide robust security for message transmission.
- Ensuring Message Confidentiality: Encrypt the messages using the recipient's public .

components

NRF24

arduino uno

Methodology

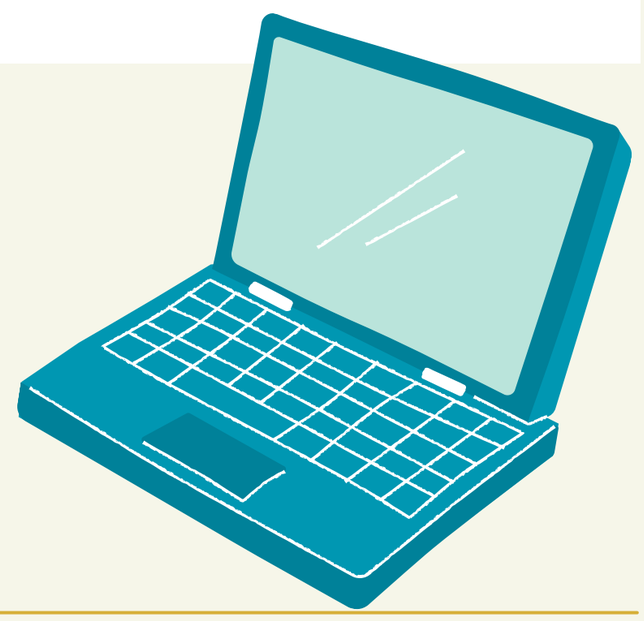
Hardware Setup:
a. Gather the required hardware components, including Arduino Uno boards, NRF24 wireless communication modules, and any other necessary peripherals.
b. Connect the NRF24 modules to the Arduino Uno boards following the wiring instructions provided by the module's manufacturer.
c. Ensure that the Arduino Uno boards are powered and connected to a computer for programming and monitoring purposes.

Software Setup:
a. Install the necessary libraries for NRF24 communication and RSA encryption.
b. start programming RSA algorithm

Generate RSA Key Pair:
a. Implement the RSA algorithm to generate an encryption key pair comprising a public key and a private key.
b. write the code to generate the key pair.
c. Safely store the private key on the receiver's Arduino Uno board.

Sender Implementation:
a. Implement the RSA encryption algorithm to encrypt the message using the recipient's public key.
b. Write the code for the sender object to send the encrypted message via the NRF24 module.

Receiver Implementation:
a. Write the code for the receiver object to receive the encrypted message via the NRF24 module.
b. Implement the RSA decryption algorithm to decrypt the received message using the receiver's private key.



Results

sender

original message:

If you can not explain it simply you do not understand it well enough

encrypted message:
vfwotrwihiwitnwdbvihjiwjnwljcviowotrwvtwitnwrivdjlnhivwjnwwdiiwditr-q

vfwotrwihiwitnwdbvihjiwjnwljcviowotrwvtwitnwrivdjlnhivwjnwwdiiwditr-q

receiver

received message:

vfwotrwihiwitnwdbvihjiwjnwljcviowotrwvtwitnwrivdjlnhivwjnwwdiiwditr-q

encrypted message:

If you can not explain it simply you do not understand it well enough

Lwhc wu urapz. Uqwlc orwlc yae uzwll rijc zcczr.

Conclusion

The project successfully developed a secure messaging system using Arduino Uno, NRF24, and the RSA encryption algorithm. The system enables the encrypted transmission and reception of messages, ensuring confidentiality and integrity. The project achieved its objectives by establishing wireless communication, implementing RSA encryption, and testing the system for proper functionality. The project's outcomes provide a reliable and efficient solution for secure message exchange between Arduino devices.