Arduino HSM Communication Project

1. Problem Identification

Secure communication between devices is crucial in environments where sensitive data is exchanged. In small embedded systems like Arduino, implementing cryptographic functions can be challenging due to limited computational resources.

The goal of this project is to create a secure hardware security module (HSM) using RSA encryption on two Arduinos to manage encrypted communication between a sender and receiver.

2. Methodology

- RSA Key Generation: The sender Arduino generates RSA key pairs (public and private) for each recipient (User B, User C, and User D).

- Key Storage in EEPROM: Both the sender and receiver use EEPROM to store and retrieve keys securely.

- Message Encryption: The sender Arduino encrypts messages using the recipient's public key before transmission.

- Message Decryption: The receiver Arduino decrypts the message using the corresponding private key, ensuring only the intended recipient can read the message.

- Serial Communication: Messages are transmitted via serial communication between Arduinos.

3. Objectives

- To design a lightweight HSM model for secure communication using Arduino.

- To implement RSA encryption and decryption within the resource constraints of Arduino microcontrollers.

- To store and retrieve cryptographic keys securely in EEPROM.

- To simulate secure communication using public-key encryption, ensuring that only designated recipients can decrypt messages.

4. Literature Survey

- Arduino and Cryptography: Previous studies and implementations of cryptographic algorithms on Arduinos have focused on optimizing algorithms to work within memory and computational limits.

- EEPROM in Embedded Security: Research has shown EEPROM's reliability in embedded systems for storing small, secure data such as cryptographic keys.

- RSA on Low-Power Devices: RSA is widely used in low-power devices for secure communication due to its asymmetric encryption scheme, which allows for secure key exchange and message encryption.