2014

Arduino to Arduino Secure Communication

2011510091 - ERFAN GHOLAMPOUR

2010510025 - AHMET OZAN EKICI

INDEX

1. Abstract

Aim of this project is to establish a secure communication between two Arduino devices. One of the devices will split input text into equal sized blocks, encrypt each block and send to the receiver device. On the other hand, the receiver device will take encrypted blocks of data, decrypt and show the received text.

2. Introduction

Arduino is a compact and simple microcontroller. Arduino has its own IDE named Arduino IDE which can be programmed with c or c++. Arduino has different libraries for different purposes. There are several libraries for different encryption methods like DES, 3-DES, AES and RSA. AES is one of the well-known and secure encryption method that is being used at almost every area. Therefore for this project AES encryption has been chosen.

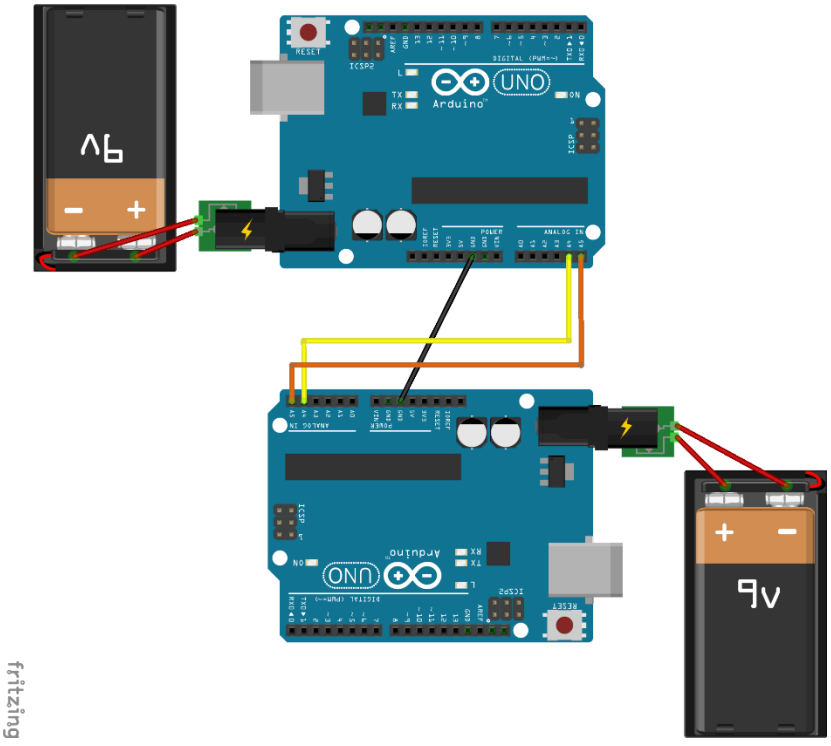
3. Related Works

There are several Arduino to Arduino communication projects without using any encryption methods. In these projects several communication methods has been used such as wire, Wi-Fi, Bluetooth, Ethernet and for each communication method advantages and disadvantages should be considered. Projects that include any encryption method are not developed to send encrypted message to another device. Encryption and decryption methods operate at one device.

4. Arduino to Arduino Secure Communication

In order to develop this project first we had to choose a method to connect two Arduino devices. We chose communication over wire considering cost and simplicity. Then to provide security for this communication we chose AES encryption method.

We used transmit (Tx) and receive (Rx) pins on Arduino to establish communication between Arduino devices. But we encountered some problems which prevented data transmission so we decided to use other digital pins for serial communication. We assigned these pins as Tx and Rx manually (Software Serial). The problem here was that last transmitted data repeated continuously. After some research we realized that there exist “wire” library that we can use for communication. The main idea for “wire” communication is that one device acts as master and other device acts as slave. Master device only sends data and slave device always receives from master device. Master device reads input from serial monitor, splits the data to blocks of 16 bytes (AES structure), encrypts and sends data block by block to the slave device. Slave device continuously listens the wire and reads incoming data char by char and sends data to decryption when reaches 16 chars. After this process decrypted data is shown at the serial monitor of the slave device.



Ahmet Ozan Ekici was responsible for master sender device and encryption.

Erfan Gholampour was responsible for slave receiver device and decryption.

5. Conclusion

We calculated the time that it takes to encrypt 1Mbit data per second and came out with results shown below.

Encryption method	Bandwidth(Mbit/s)
AES	0.21
RSA	0.06

Standards	Bandwidth(Mbit/s)	AES	RSA
802.11a	6 - 54	X	X
802.11b	1 - 11	X	X
Bluetooth 1.2	1	X	X

According to results we came to the conclusion that sending data over Wi-Fi and Bluetooth standards is not logical while using AES or RSA encryption.

6. References

- http://arduino.cc/en/Tutorial/MasterWriter
- http://robotic-controls.com/learn/arduino/arduino-arduino-serial-communication
- https://github.com/DavyLandman/AESLib