**Course Projects**

**Automotive Cybersecurity for Automotive Technicians**

The purpose of these projects is to demonstrate your familiarity with the course tools introduced in the course Experiments.

**Project 1: Emulating a CAN Signal**

This project will focus on connecting two microcontrollers (namely, a pair of Photon Wi-Fi IoT boards) together using the CAN bus by using an AND gate. You will need to obtain two Photon devices and an AND gate chip (some suggestions are listed below), along with some jumper wires and a breadboard.

There must be at least two (2) nodes on the CAN bus in order for it to work, due to the way it is designed and how messages are acknowledged. So no, you cannot wire the CAN TX to the CAN RX.

If you use a 7408 2-input AND, you will not need to wire any unused inputs. If you use a 7421 4-input AND gate, you will need to wire unused inputs to power.

You will also need a 220 Ω resistor, a green LED, and a pushbutton switch. This system will allow you to flash the CAN code that you will write to each Photon board.

**Extra Credit:** Make a custom AND gate with transistors you have or that you buy.

In addition to purchasing and wiring the components, you will need to write CAN receiver and CAN transmitter code to be flashed to the respective Photon board.

Here is what you may need for the project, depending on your setup:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Part Name** | **Link** | **Quantity** | **Piece Cost** | **Total Cost** |
| PHOTONH Development Board | [HERE](https://www.amazon.com/Particle-Reprogrammable-Development-Prototyping-Electronics/dp/B016YNU1A0) | 2 | 19.00 | 38.00 |
| 7408 Quad 2-Input AND Gate | [HERE](https://www.jameco.com/webapp/wcs/stores/servlet/ProductDisplay?storeId=10001&productId=49146&catalogId=10001&langId=-1&CID=GOOG&gclid=EAIaIQobChMIybCe97_74QIVEb7ACh1ElgZ2EAQYASABEgKaj_D_BwE) | 1 | 2.95 | 2.95 |
| 7421 Dual 4-Input AND Gate | [HERE](https://vetco.net/products/nte7421-ic-ttl-dual-4-input-and-gate?gclid=EAIaIQobChMI567Zk8D74QIVWv_jBx2BdAC9EAkYAiABEgL3X_D_BwE) | 1 | 2.24 | 2.24 |
| **Note: Only purchase one (or none) of the AND gates.** |  |  | **Total Cost:** | 43.19 |

**Project 2:**

RF Key fob Hacking

**Background Information**

To obtain background information on RF signals and how devices use them, please read the following webpage. Much of the fundamental aspects of this project are based on this tutorial. In this project, we will be conducting some of the analysis the author of the article does to determine the signal data that our key fob emits.

[Link to guide](https://arduinobasics.blogspot.com/2014/06/433-mhz-rf-module-with-arduino-tutorial_27.html) [<https://arduinobasics.blogspot.com/2014/06/433-mhz-rf-module-with-arduino-tutorial_27.html>]

**List of Required Materials:**

* 2x Arduino Unos
* 2x 335 Mhz RF Receiver Boards
* 1x 335 Mhz RF Transmitter Board
* 1x Push button switch
* 1x Green LED
* 1x 330 Ohm Resistor (Orange, Orange, Brown, Gold)
* Wires of various lengths and colors
* 1x Large or 2x small bread boards
* 1x 12 volt 0.5 amp wall plug power supply
* 1x USB cable for Arduino Uno

**Assembly Instructions**

1. Follow the wiring guide on the following page. All of the information needed to make the boards for this project should be included there and in the following notes:

*Important Notes:*

1. Pins 1 and 3 of the push button switch are wired together. This is on purpose and is needed to detect the key press in the code for the hacker board.

Hacker Board Assembly Notes:

1. Data pin next to the Vcc pin on the receiver is connected to pin 2.
2. Push button switch next to the receiver is connected to pin 6.
3. Push button switch next to the transmitter is connected to pin 5.
4. Data pin of the transmitter is connected to pin 10.
5. All devices are powered by a common 5v pin from the Arduino board.

**Wiring Guides for the Receiver and Hacker Boards**

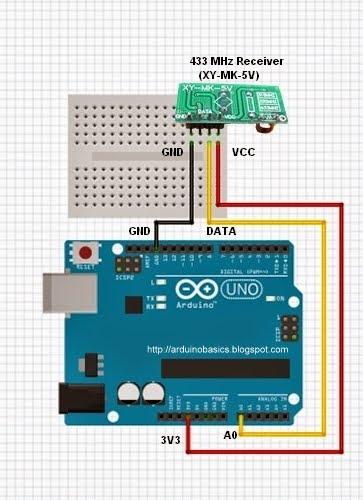


Figure 1: Receiver Board Layout [https://bit.ly/2W076FX]

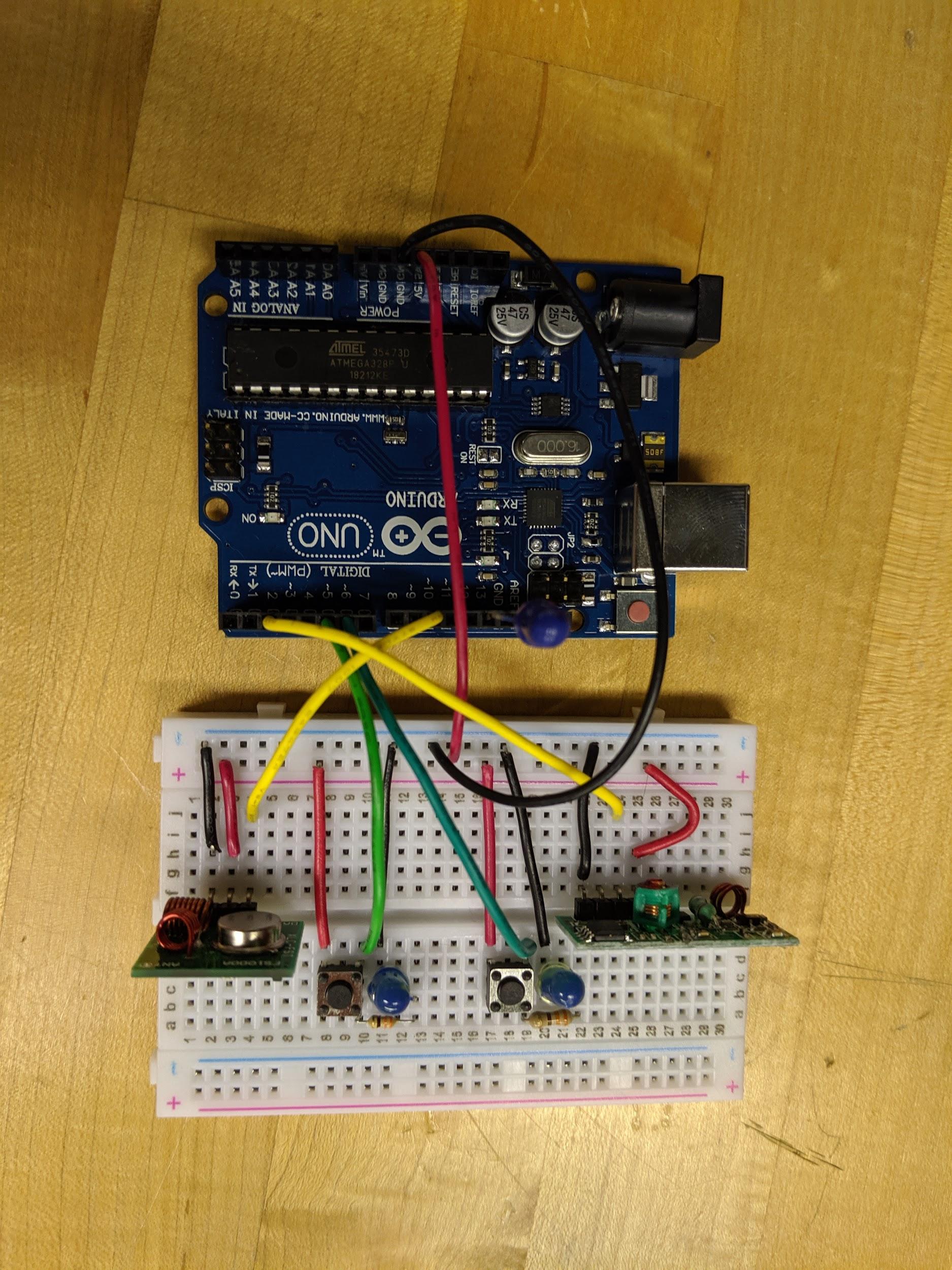


Figure 2: Hacking Board Layout

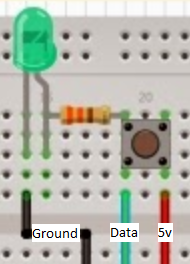


Figure 3: Wiring diagram for each push button [https://bit.ly/2W076FX]

**Part 1: Decoding the RF Signals**

In this section of the lab you will be decoding the signals emitted from the key fob. Follow the instructions below and answer the questions. Refer back to the blog web page for assistance if needed.

Procedure:

1. Flash the “Receiver\_Part1” onto the receiver Arduino board.
2. Open the Serial Monitor in the Arduino IDE (Tools > Serial Monitor).
3. Press one of the buttons of the key fob.
4. The data read from the RF receiver will print out in the Serial Monitor window.
5. Copy the data from the Serial Monitor and paste it into Excel or Google Sheets.
   1. If you cannot paste directly then paste the data into a text file first.
   2. Delete the header on the data (Highlighted below) and save the file as a “CSV”.
   3. You can now import the CSV file into Excel or Google Sheets.
6. Using either Excel or Google Sheets trim your data down to the transmission section. Refer to the blog post to see what this should look like.
7. Fill out the table below with your signal and answer the questions.
8. Show results to the professor before moving on.

**Table 1: Signal Analysis**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Low |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| High |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Low (cont.) |  |  |  |  |  |
| High (cont.) |  |  |  |  |  |

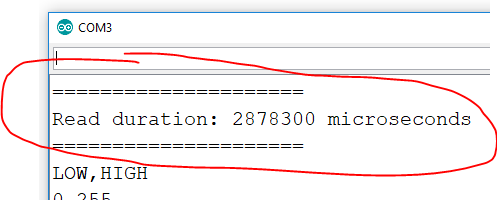


Figure 4: Highlighted header text to be deleted

**Part 2: Hack the fob!**

In this section you will be using both Arduino boards to hack the key fob. Instead of analyzing the raw frequency changes of the RF we will be using an encoder/decoder called RCSwitch. If you have not added the library to your Arduino IDE you need to do so before proceeding any further in this lab. Instructions on how to do this are below.

Adding Libraries to Arduino IDE

1. In a sketch click on “Tools” then select “Manage Libraries”
2. In the filter type “RCSwitch”.
3. Click Install.
4. Restart Arduino IDE.

The following changes need to be made to the set up for this to work properly.

* On the receiver board move the data pin from pin A0 (Analog) to pin 2 (Digital).

Procedure:

1. Flash the “RC\_RX\_1” code file onto the receiver board.
   1. Unplug the receiver board from your computer and connect to the wall for power using the wall power supply. This is not necessary but it does help remove any confusion when flashing the hacker board.
2. Test the key fob to see if it correctly turns the LED on the receiver board on/off.
3. Complete the missing code in the “RC\_TX\_1” and compile it until there are no errors.
4. Flash the “RC\_TX\_1” code file onto the hacker board.
5. With both of the boards powered, open the Serial Monitor for the hacker board and put it into recording mode (Button 1 next to the RF transmitter).
6. Press the desired button on the key fob.
7. The signal should be recorded. Now you should be able to control the LED with the transmit button on the hacker board.
8. Redo the recording by resetting the hacker board and trying different buttons on the key fob.
9. Demonstrate your setup to the course instructor before leaving the lab.