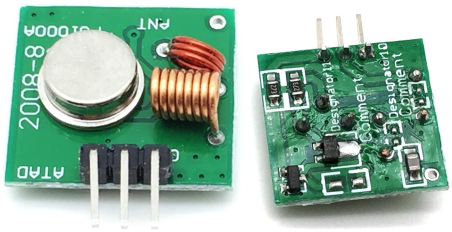
About

Vulnerable radio protocol for security demonstrations.

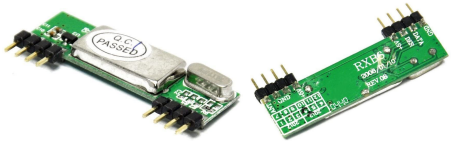
Two software components are in use: The radio sending part: send_data The radio receiving part: receive_data

Material used

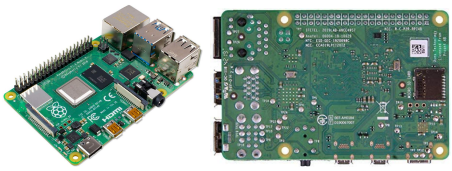
FS1000A - 433 MHz Transmitter module



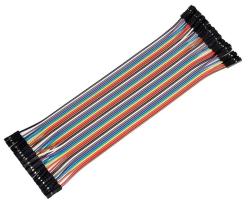
RXB6 - 433 MHz Receiver module



RPi4 - Receive/Transmit command and SDR processor



Dupont Wires - Signal and power wiring cable



RTL-SDR dongle - Software Defined Radio receiver

This equipement will be used later on in the training.

Wiring

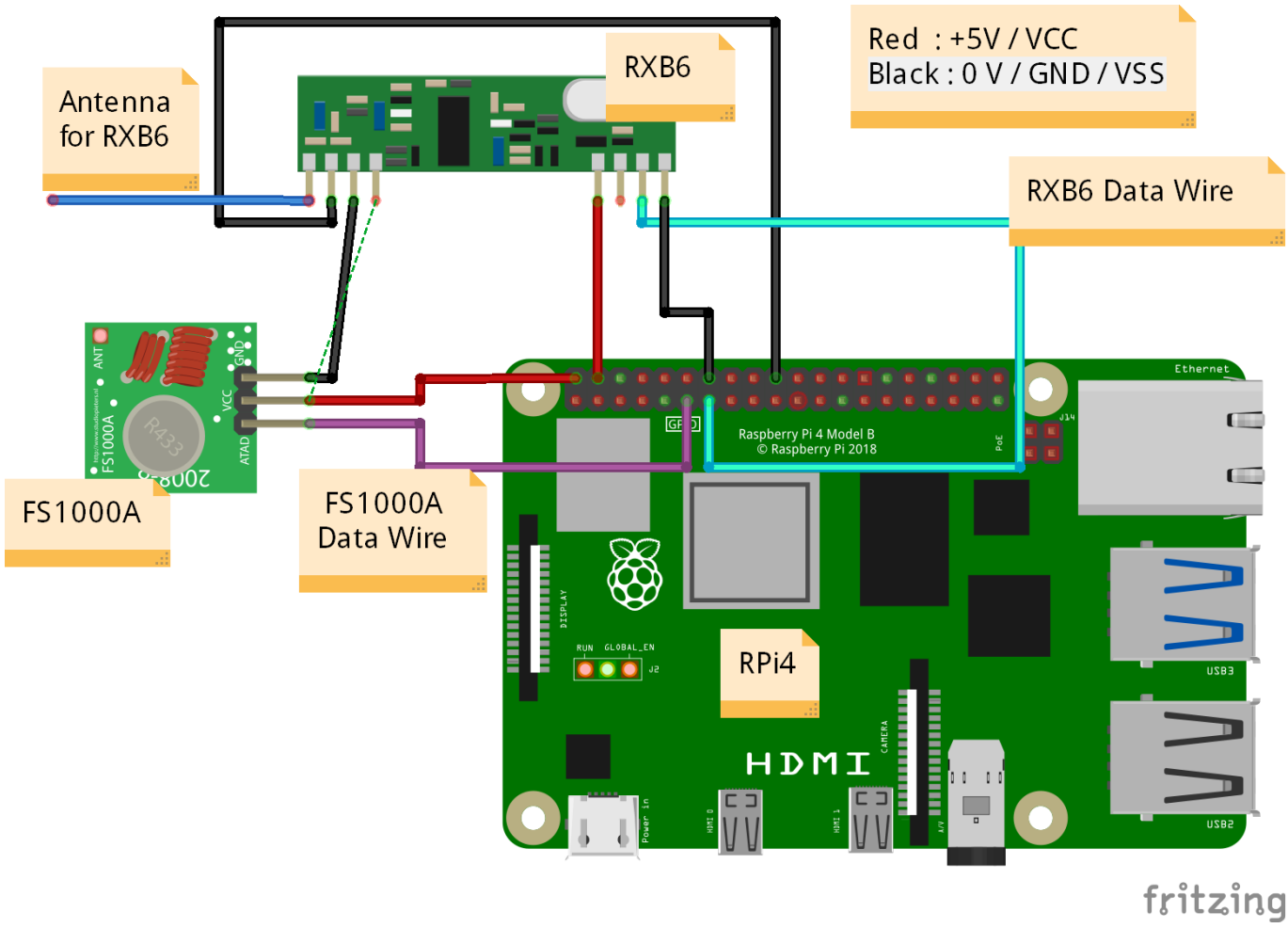
Personal Safety:

No need to worry we will wire safe to use voltages and currents so do not be worried too much about your own safety.

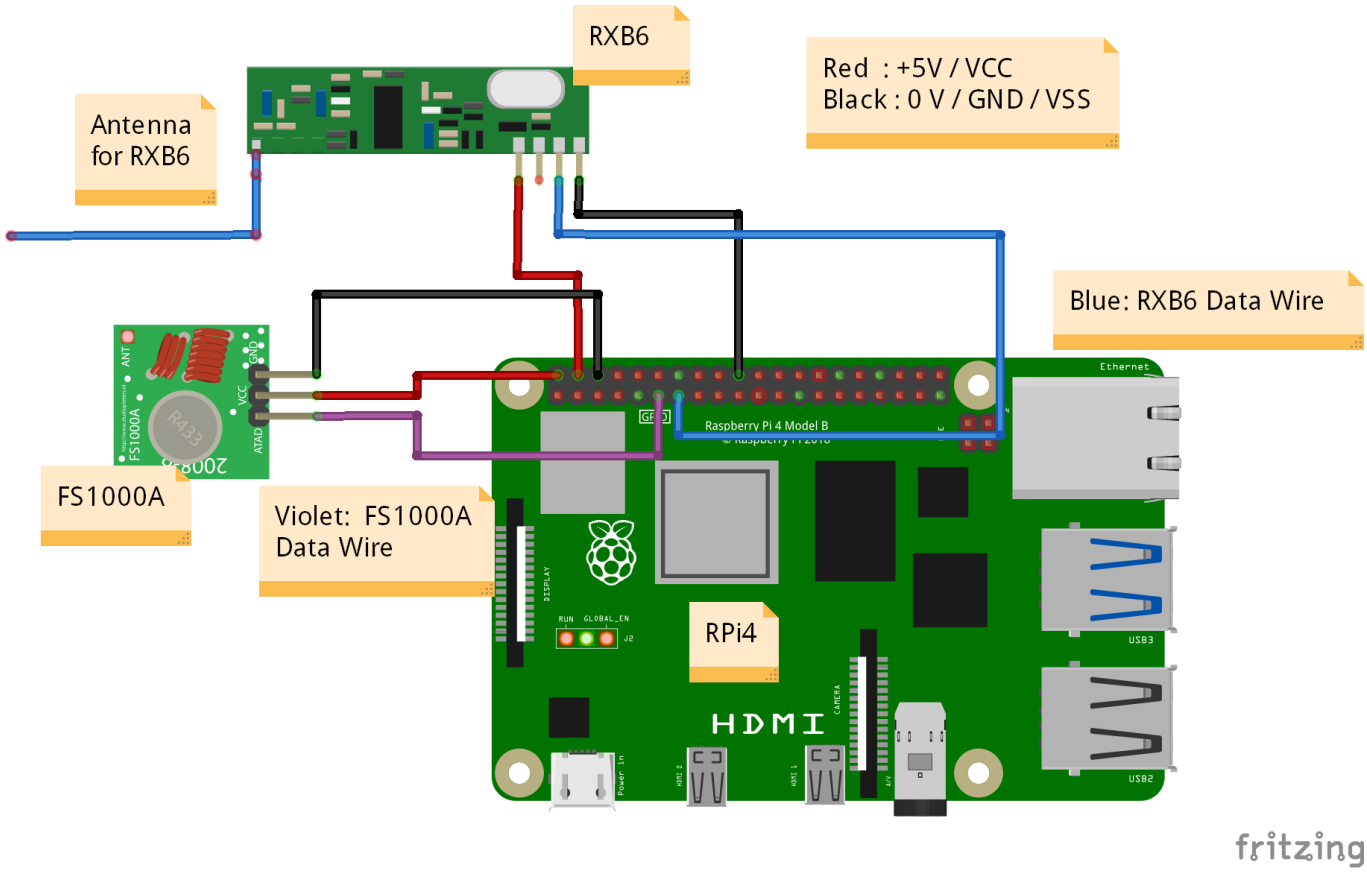
Circuit safety:

- Do not wire 5V to 0V as this will cause a short circuit and destroy your components / processors.
- Do not let the circuits touch each other

On a 8 pin RXB6



On a 4 pin RXB6



Power lines
Red : +5V / VCC
Black : 0 V / GND / VSS

Signal lines
Cyan : RXB6 Data => RPi4 GPIO 27 (pin 13)
Blue : Antenna for RXB6 (Connect only to RXB6)
Purple : FS1000A Data =>RPi4 GPIO 17 (pin 11)

```
J8:
   3V3  (1) (2)  5V
 GPIO2  (3) (4)  5V
 GPIO3  (5) (6)  GND
 GPIO4  (7) (8)  GPIO14
   GND  (9) (10) GPIO15
GPIO17 (11) (12) GPIO18
GPIO27 (13) (14) GND
GPIO22 (15) (16) GPIO23
   3V3 (17) (18) GPIO24
GPIO10 (19) (20) GND
 GPIO9 (21) (22) GPIO25
GPIO11 (23) (24) GPIO8
   GND (25) (26) GPIO7
 GPIO0 (27) (28) GPIO1
 GPIO5 (29) (30) GND
 GPIO6 (31) (32) GPIO12
GPIO13 (33) (34) GND
GPIO19 (35) (36) GPIO16
GPIO26 (37) (38) GPIO20
   GND (39) (40) GPIO21
```

Software Usage

Two software components are in use:

- For radio transmission: send_data
- For radio reception: receive_data

1 - Prepare your terminals

Two terminals are needed in order to have a complete view of the two applications: A data sender, a data receiver, and a spare terminal for work.

You can use the following tmux command to split your terminal pane. See tmux cheatsheet below for more help.

```
tmux new-session \; split-window -h \; split-window -v \; attach
```

2 - receive_data

The receive_data program does not take any parameters and waits forever for incomming radio frames.

Type the following into any of the three terminals

```
taskset 0x1 ./receive_data
```

3 - send_data

The send_data program can take up to 5 arguments: if none is provided, default values are used, if [command, argument, value, login, password] are provided, they are used.

Example:

```
    send_data PRINT TMP 2200 control0 P@$$w0rd
```

All fields are fixed-length:

```
    Command: 5 Bytes
    Argument: 3 Bytes
    Value: 32 bit integer
    Login: 8 Bytes
    Password: 8 Bytes
```

For the exercice use this command in any of the two remaining terminals

```
while [ 1 == 1 ];do taskset 0x2 ./send_data PRINT TMP $(($(vcgencmd
measure_temp|grep -o '[0-9]*\.[0-9]*'|sed 's/\.//g')*10)) control0 P@$$w0rd;sleep
1;rm data_to_print.txt; done
```

TMUX Cheatsheet

- Split H/V
    - To split horizontaly Ctrl+b then "
    - To split horizontaly Ctrl+b then %
- Move to another pane
    - Ctrl+b then arrow
    - Ctrl+b then arrow
- make pane larger / smaller
    - Ctrl+B then keep ALT pressed + Up/Down/Left or Right (repeat possible)

- Scroll
    - Ctrl+B then [then Up/Down/Left/right
- Close pane
    - type exit
      or
    - Ctrl+b then :x then confirm with y
- Copy mode => CTRL+b
    - Scroll up or down :Go into copy mode (Ctrl+b) then use arrow keys
    - Select :Go into copy mode (Ctrl+b and the [ ) then press (Ctrl+space)
    - copy to TMUX buffer : Go into copy mode (Ctrl+b), select (Ctrl+space) then press copy (Ctrl+w)
    - Paste :Go into copy mode (Ctrl+b) and paste (]) after having copied of course
    - Other commands https://gist.github.com/MohamedAlaa/2961058