USAF ACADEMY
DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING
LESSON 17 LAB - RF REVERSE ENGINEERING
Lab Packet
Spring 2027

Name: _____ **Section:** _____ **Date:** _____

Learning Objective 6.6: I can perform RF reverse engineering on an unknown signal: identify its modulation, symbol rate, and payload structure.

This packet is the L17 Lab, in three parts, and you turn it in once, complete, before Lesson 18. Do **Part 1** on your own before the lab period: read the recording's meta file, check `L17-chips.grc` on the lesson's recording, and work out the chip settings. **Part 2** is what you find, build, and observe, recorded in class: Questions 4 to 7 on your own laptop, Question 8 at a PlutoSDR station with your team, and Question 9 with a real remote of your choice. Do **Part 3** on your own after the lab: explain, in words, the evidence for each answer.

Grading. You submit the packet once, we grade it against Objective 6.6 on the course's 1 / 0 scale, and you may revise it under course policy. Paste screenshots where a question asks for one.

The device. The recording `L17-lab-unknown.sigmf-data`, with its `.sigmf-meta` file, is on the L17 Lab page. It is a Simulated remote outlet switch with six buttons, pressed once each in the order the meta file lists. Nothing else about it is given: finding it out is the lab.

Transmitting. In class we transmit only into a cable, into a shielded enclosure, or at very low power in an ISM band, and only when the lesson says to. This device's band is an FCC Part 15 frequency, not a U.S. ISM band, and a signal the course makes never goes out on the real device's frequency: your encoder transmits at 915 MHz, in the 902 to 928 MHz ISM band. Questions 1 to 7 run on your laptop and transmit nothing. Question 8 transmits from a PlutoSDR's TX port, through a cable with an inline 30 dB SMA attenuator, to a second PlutoSDR's RX port, or, if your instructor says so, over the air at 915 MHz at low power. Connect the cable and attenuator before you run the flowgraph, and connect an antenna only when your instructor says so. Never set TX attenuation below 30 dB or change the slider's range; a Pluto's input is rated to only a few dBm. We have compiled the PlutoSDR flowgraphs but not run them on a radio, so Question 8 is their first run on hardware. Question 9 only receives, which is always allowed.

Part 1: Pre-Lab (individual, before the lab period)

1. **The meta file.** Open `L17-lab-unknown.sigmf-meta` in a text editor.

   (a) Record the recording's datatype, sample rate, and center frequency.

	Datatype	Sample rate	Center frequency
`L17-lab-unknown`			

   (b) Give the values you set for `rec`, `samp_rate`, and `fc` in `L17-sigmf-view.grc`, and the Output Type of its SigMF Source.

   (c) Paste a screenshot of the viewer running on this recording.

2. **Reading chips in GNU Radio.** Open the lesson's recording, `L17-fan-remote.sigmf-data`, in `L17-chips.grc`, with `samp_rate` 200000, `fc` 350e6, and the carrier offset at 40000 Hz.

   (a) Measure the shortest pulse on the envelope, and set the chip length to it. Record the chip length in samples and in microseconds, and the first line of chips the Chip Reader prints, with its pause.

   (b) Paste a screenshot of `L17-chips.grc` running on the recording.

3. **Samples per chip.** The Chip Reader's chip length and your encoder's `chip_len` are both a chip's length in samples. Fill in the table for each chip length at this recording's sample rate, from Question 1(a), and at the PlutoSDR flowgraph's 1 MS/s.

Chip length	240 μs	300 μs	600 μs	1 ms
At the recording's rate				
At 1 MS/s				

Part 2: Measurements (in class)

4. **Step 1: the carrier.** Follow the lab page's steps for `L17-sigmf-view.grc`.

   (a) List every signal on the waterfall, its frequency, and whether it bursts or stays on. Say which one is the device, and why.

   (b) Record the carrier offset: the center of the bursts on the Frequency Sink or waterfall, checked as the midpoint of the half-height offsets on the envelope. Paste a screenshot of the window at that offset.

   (c) Record the device's carrier frequency.

5. Steps 2 and 3: modulation and encoding. Follow the lab page's steps in `L17-chips.grc`.

(a) Record the shortest pulse you measured on the envelope, in samples and in microseconds, and the chip length you set.

(b) Record the shortest gap you measured, in samples and in microseconds. Say whether it fits your chip length, and how you checked that the Chip Reader's lines repeat from burst to burst.

(c) Name the modulation and the encoding. Give the evidence for each from the envelope and the lines of chips, and describe any structure in each burst besides the data bits, if there is any.

(d) Find the baud rate, in chips per second, and the bit rate, in data bits per second.

	Baud rate	Bit rate
The device		

6. Step 3: the fields.

(a) Decode one burst of each button and write its data bits in hex.

1 On		2 Off	
1 Off		3 On	
2 On		3 Off	

(b) Mark the fields: which bits never change, which change with the button, and any field that follows neither. If you find such a field, give the rule it follows and check it on two buttons.

(c) How many times does one press send its frame, and how long is the pause between frames?

7. **Step 4: build the encoder.** Start GRC with an empty canvas. Do not open `L17-fan-tx-sim.grc`: build the encoder yourself as the lab page lists, with your settings from Questions 4 to 6.

   (a) Paste a screenshot of your flowgraph's canvas, and the lines of chips `L17-chips.grc` prints for `my-unknown.sigmf-data` and for the original recording, for the same button.

   (b) Do the same for a second button, and say whether every chip matches.

   (c) Record the noise amplitude at which the Chip Reader's lines of chips from your recording first stop matching the original, and describe what goes wrong first.

8. **Step 5: transmit into a cable.** At a PlutoSDR station, with your team, follow the lab page's steps: connect the first Pluto's TX port to the second Pluto's RX port through the 30 dB attenuator, set `fc` to 915e6 and run `L17-capture.grc` on the second Pluto, and run your Pluto encoder at 915 MHz. When you finish, stop both flowgraphs and unplug the radios before you disconnect the cable.

   (a) Paste a screenshot of both windows with your signal on the capture flowgraph's waterfall.

   (b) Open `capture.sigmf-data` in `L17-chips.grc` at the sample rate and center frequency in its meta file, 1 MS/s and 915 MHz, and compare its lines of chips with the original recording's for the same button.

   (c) Record whether the chips still match at each TX attenuation, and explain in words, from what you saw on the waterfall and in `L17-chips.grc`, what limits the link as the attenuation rises.

TX attenuation (dB)	60	70	80	89
Chips match?				

9. A real remote (receive only). Follow the lab page's steps with a real key fob, doorbell, or sensor of your choice. Answers depend on the device.

(a) Name the device, and record its carrier frequency and how you found it: the spectrum of `L17-explore-pluto.grc`. Paste a screenshot.

(b) Record the modulation, the chip length, and the encoding, with the evidence from `L17-chips.grc` for each.

(c) Compare the recordings of two buttons, and of two presses of the same button. Say which bits change, and whether a press repeats the same frame each time.

Part 3: Writeup (individual, after the lab)

10. Analysis.

(a) For each of the carrier, the modulation, the encoding, and each field, give the observation that settled your answer: what you saw on the waterfall, the envelope, or the lines of chips, and which comparison between buttons identified each field.

(b) From your Question 6 table and your noise run in Question 7(c), explain how a receiver of this device could tell a frame damaged by noise from a good one, and what kinds of damage it could miss.

(c) Explain why your encoder from Question 7 would operate a device that matched this recording, and describe in words how a rolling code, as in a car key fob, would stop a recording of one press from being reused.

Documentation: _____