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

Show your work. Write a **Documentation** line at the end (**None** if you did not collaborate).

1. **Finding the carrier.** A Simulated wireless doorbell is recorded at 1 MS/s, centered at 314.900 MHz, which is an FCC Part 15 frequency. Opened in a viewer like `L17-sigmf-view.grc`, the waterfall shows a narrow line 150 kHz below the center that stays on the whole recording, and short bursts 80 kHz above the center that appear each time the button is pressed.

   (a) Find the doorbell's carrier frequency, and say how you know which signal is the doorbell.

   (b) Give the Frequency Xlating FIR Filter's Center Frequency that shifts the doorbell to 0 Hz.

   (c) The bursts look several kilohertz wide on the spectrum, and the steady line looks almost as thin as one FFT bin. In words, explain why.

2. **The meta file.** A teammate sends a SigMF recording. Its `.sigmf-meta` file holds these lines:

```
"core:datatype": "ci16_le",  "core:sample_rate": 2000000.0,  "core:frequency":
                                    433000000.0
```

(a) Give the SigMF Source (Minimal) block's Output Type, the block that must follow it, and the flowgraph's `samp_rate` and `fc`.

(b) `ci16_le` stores each sample as two 16-bit numbers. How many bytes does a 5 s recording take, and how many would `cf32_le` take?

(c) The SigMF Source (Minimal) in `L17-chips.grc` has its Output Type set to complex float (`fc32_le`). Explain in words what the flowgraph would show if you opened this `ci16_le` file without changing it.

3. **Chips to bits.** `L17-chips.grc` opens the doorbell's recording at 1 MS/s with a chip length of 300 samples, and its Chip Reader prints every burst as the same line of chips:

```
1000100010101010001010001
```

   (a) Find the chip length in microseconds.

   (b) Every pulse is one chip long, and the gaps after the pulses are one chip or three chips. Name the encoding, and explain why the line ends with a lone pulse.

   (c) Take a long gap, `1000`, as a 1 and a short gap, `10`, as a 0. Decode the line into 8 bits and write them in hex.

   (d) Find how long this frame lasts, and explain in words why a pulse-distance remote has no single bit rate.

4. **Encoder settings.** A Simulated garage remote uses pulse-width coding with 4 chips per bit, `1110` for a 1 and `1000` for a 0, with 350 μs chips. Each frame is 12 bits followed by 10 ms of silence. You build its encoder as the L17 lesson did, at $f_s = 1$ MS/s: a Vector Source of the bits, a Map, Unpack K Bits, Char To Float, a Repeat, and a Stream Mux with a Constant Source of 0.

   (a) Give the Map's table and Unpack K Bits' K.

   _____; K = 4][0cm]

   (b) Give the Repeat's interpolation and the Stream Mux's two lengths.

   _____][0cm]

   (c) Your encoder's output, opened in `L17-chips.grc` beside the original recording, shows the same lines of chips except that every one of yours is 4 chips longer. In words, give the most likely mistake.

5. **Which modulation?** Four unknown recordings open in a viewer like `L17-sigmf-view.grc`. Name the modulation of each from what the displays show, and say which lesson's signal it resembles.

   (a) The waterfall shows two parallel tracks a few kilohertz apart, and the signal is always on one of them; the envelope is constant.

   (b) The waterfall shows one band that stays on and does not move, and the envelope is nearly constant; a constellation plot after carrier recovery shows four clusters.

   (c) Short bursts appear at one frequency, and the envelope switches between zero and one level in pulses of two lengths.

   (d) Short dashes of the same width appear at a new frequency every few hundred milliseconds, stepping around a band.

6. **Repeats and noise.** The L17 fan remote sends each frame 6 times per press and ends each frame with a check nibble.

   (a) In words, explain what the repeats and the check each let a receiver do when the signal is weak.

   (b) You lower the signal in the pulse decoder explorer by raising the noise. Name two things you would watch to see the frames start to fail, in the explorer or in `L17-chips.grc`.