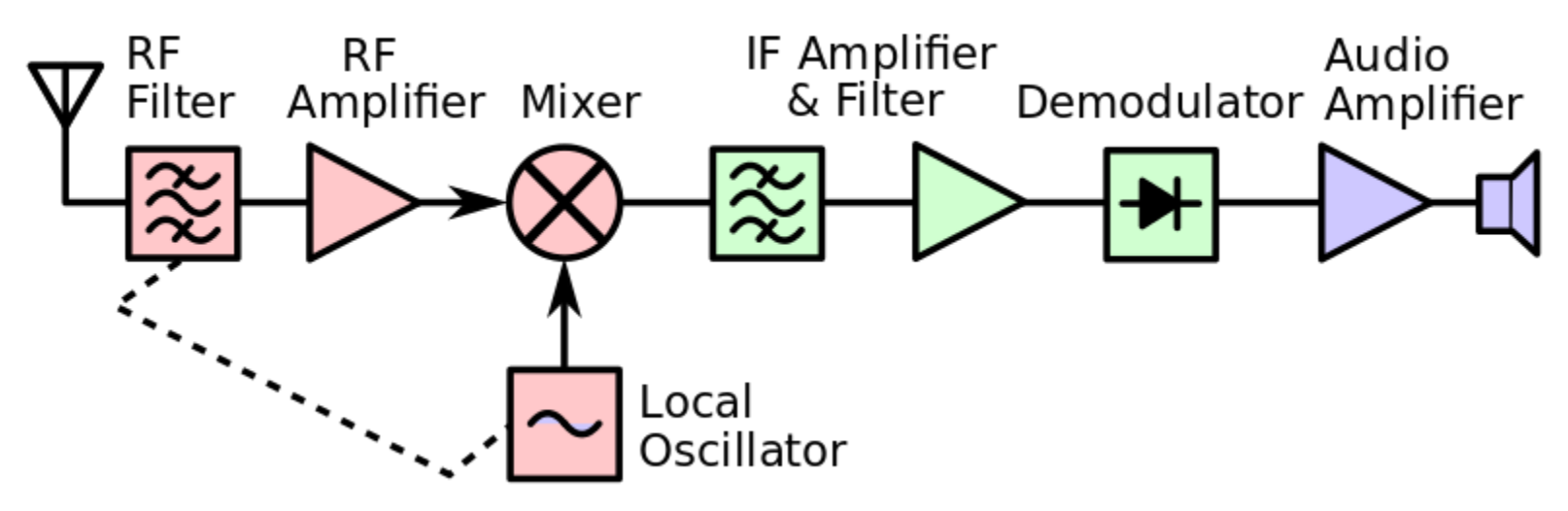
OVERVIEW OF SOFTWARE-DEFINED RADIO

- Traditional radios consist of many hardware components:
  - Mixers: Combine signals
  - Filters: Reject/amplify select components of signals
  - Amplifiers
  - Modulators / Demodulators (modems): "Decode" a signal into a useful format

OVERVIEW OF SDR (CONT.)



- Traditionally analog, which is expensive
- What if we could do all of the tasks in software? *We can with software-defined radio*

RTL-SDR

- Very inexpensive ($10-$30) USB dongle SDR
- Gives us the RF front end to our PC to interface with GNU Radio
- Only receives, can't transmit

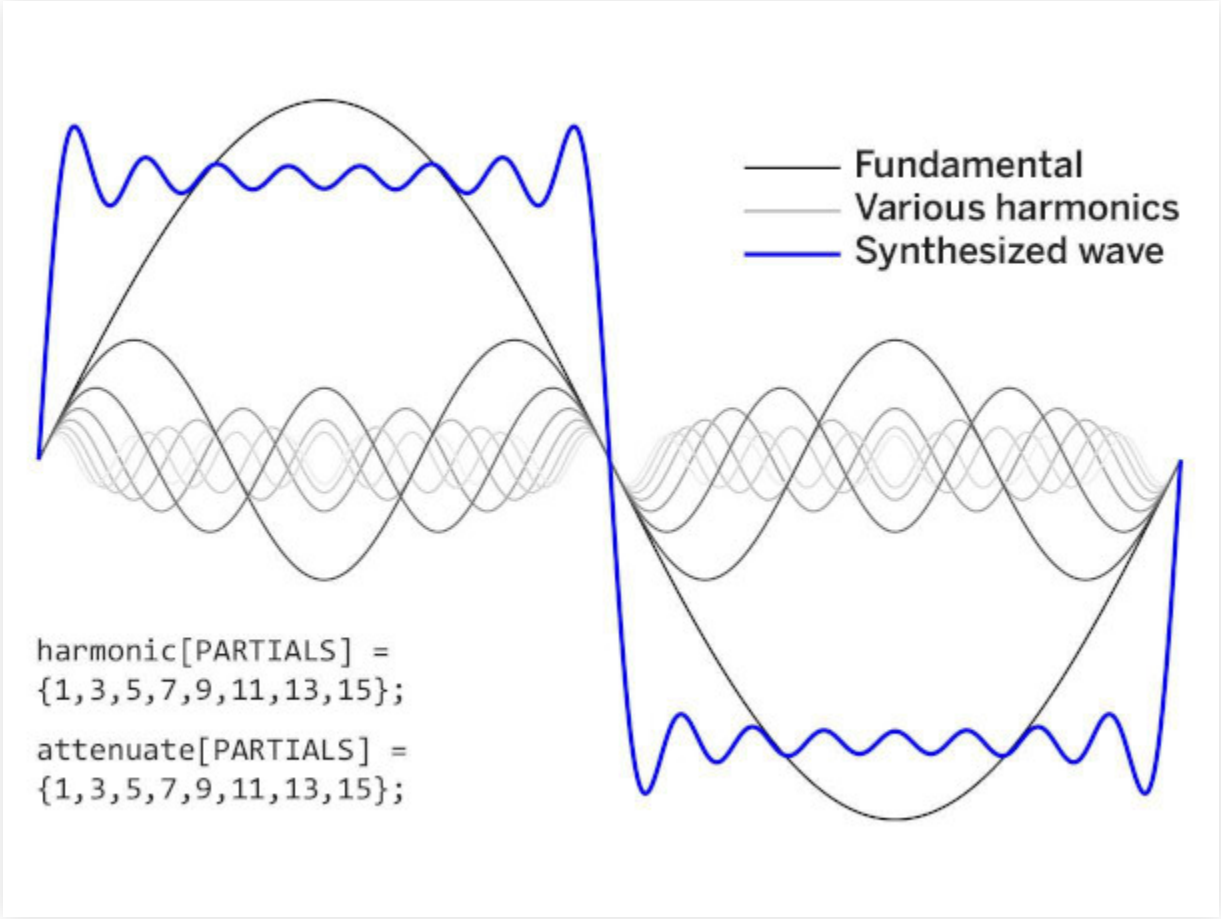
OVERVIEW OF RPITX

- RF transmitter for the Raspberry Pi
  - Only transmits, can't receive
  - If we pair this with an RTL-SDR, we have a full Rx/Tx pair!
- How does it work?
  - RPi's clock generator set to output to a GPIO pin with an "antenna" connected
  - Clock generator frequency is changed thousands of times a second to generate an RF signal

OVERVIEW OF RPITX (CONT.)

- What are it's downsides? (e.g. Why spend $300 on a HackRF if I can just use this?)
  - Beta quality software - even doing something as simple as disabling automatic logic on the RPi broke transmission
  - Very limited output power
  - **Harmonics**

A (VERY) BRIEF EXPLANATION OF WHY WE HAVE HARMONICS



RPITX DISCLAIMER

- LPD433: Internationally recognized frequency band from **433.050 MHz to 434.790 MHz**
  - A license is *not* required to use this band, as long as transmissions are below 10 mW
- If you don't have a filter on your RPi antenna output, you will be transmitting in all harmonics of this frequency as well

OVERVIEW OF REPLAY ATTACKS

- Similar to a man-in-the-middle attack, except you're rebroadcasting the *same* information instead of modifying it
  - Commonly used maliciously to impersonate key fobs to gain access to garage doors, cars, etc.
- We'll be using this today in a non-malicious manner by impersonating remotes for 433 MHz home automation devices

LIVE DEMO OF GNU RADIO INTERCEPTING A TRANSMISSION

ANALYSIS OF RECORDING

- Modulation: Amplitude Shift Keying (ASK)

LIVE DEMO OF A REPLAY ATTACK

OTHER OPEN SOURCE SDR PROJECTS

- Skywave Linux
- sdr.hu (check if OSS)
  - KiwiSDR
  - OpenWebRX
- Home Assistant (for tie-in with other devices, make an open source smart home)
- Huginn (open source IFTTT)