Motivation:
The motivation of our project is to do a proof of concept for the AIR-FI research. The AIR-FI paper is about exfiltrating data from air-gapped computers via Wi-Fi signals. The basic idea is that electromagnetic signals generated by the RAM of a computer can be intercepted and decoded by nearby Wi-Fi capable devices using the physical layer information exposed by Wi-Fi chips. This was proven using air gapped computers in the paper, however we would like to show that it can be done on different hardware. Instead of using electromagnetic signals from an air-gapped computer, we will use the electromagnetic signals emitted from the RAM of a PC.

Design Goals:
We plan to use a PC as our main hardware component. We will be encoding and intercepting electromagnetic signals from the PC's RAM by using Sparkfun Wi-Fi chips. We will overclock the PC's RAM to reach the Wi-Fi frequency of 2.4GHz. Once signals are intercepted, they will be sent to a nearby Wi-Fi capable device. Once sent to the device, the EM signals will be decoded by performing FFTs on said signals which will output the desired information.

Deliverables:
- Proof of concept of AIR-FI research but on a PC
- Study demodulation techniques to explore the most optimal option
- Present empirical results on communication range and data transfer rate

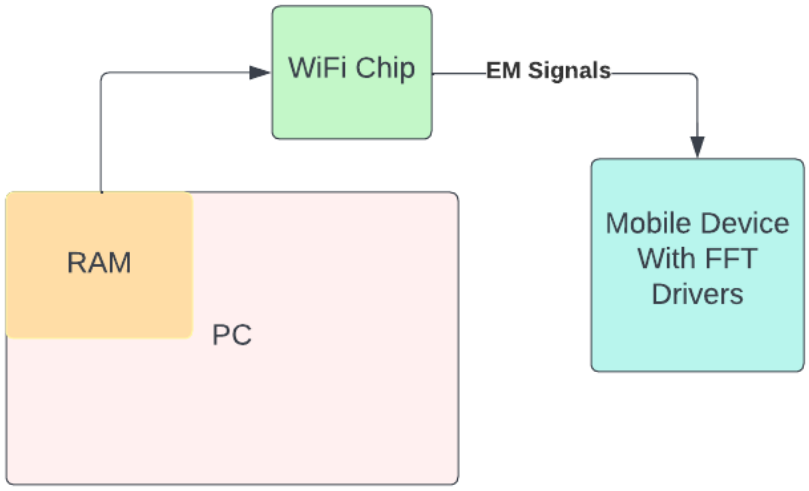
Challenges:
Some challenges we expect to face are overclocking the RAM to reach the WiFi bandwidth of 2.4GHz safely, making sure no application interrupts the demodulation process, and successfully extracting the test signal from any noise.

HW Requirements:
- Wi-Fi Chip
- RAM
- A device that could obtain a stream of data from the WiFi Chip.

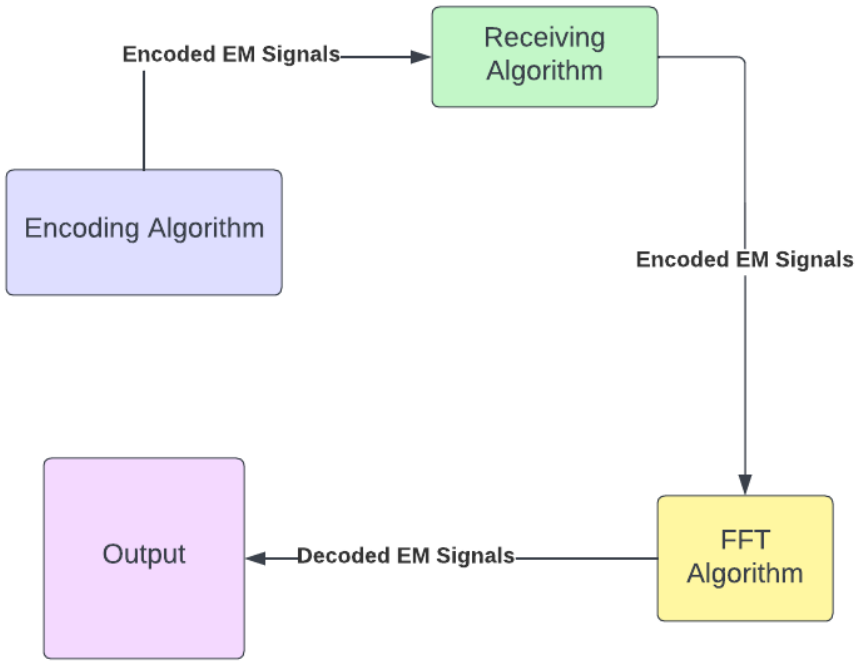
SW Requirements:
- Encoding algorithm
- Receiving Algorithm
- FFT Algorithm

Block Diagrams:

HW:



SW:



Team Members/Roles:
Khadija Ben-Neticha - Hardware
Nathan Costa - Software
Yanbin Wu - Research

Timeline:

Goal:	Expected Date:
Submit Proposal	9/29
Find device FFT drivers/research	10/6
RAM Software Development/testing	10/13
Wi-Fi Module Testing/RAM Software testing	10/20
FFT on Wi-Fi Module Development	10/27
Development/Testing of FFT and receiving Algorithms	11/03
Testing of complete system/Check-in	11/10
Final Testing/Wrapping up	11/17
Thanksgiving Break	11/24
–Buffer–/Check-in	12/1
Demonstration	12/8
Final Report	12/20

References:
1: Natural timestamping using powerline electromagnetic radiation, ACM Transactions ’18

2: Low-power Clock Synchronization using Electromagnetic Energy Radiating from AC Power Lines

3: Air-Fi: Leaking data from air-gapped computers using Wi-Fi frequencies