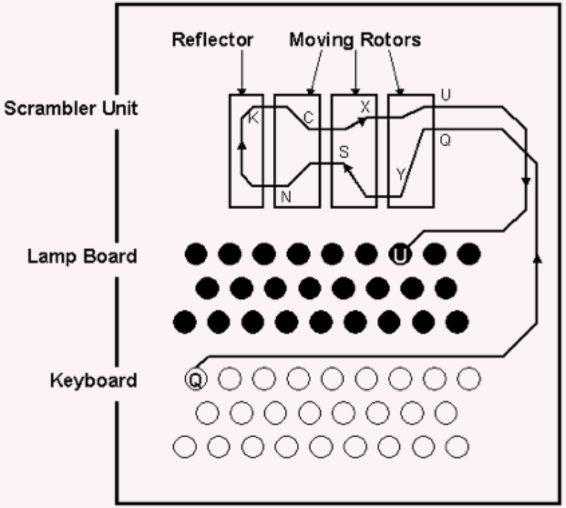
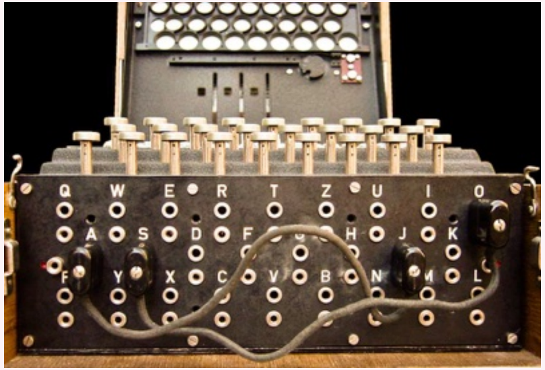
B5: Enigma18

Nancy Anderson
Amelia Lobo
Tanisha Sethi

- Cipher device, similar to a typewriter, used by Germany during WWII
- Rotor system that altered encryption each time message was sent
- Historically, would pick 3 out of 5 rotor options





Use Case

- Mimic the look and feel of historic Enigma machines with a modern take
- Educate about cryptography through hands-on encryption and decryption
- Designed for use in museums and classrooms (open-source)
- **Existing solutions:** electromechanical (historical, but heavy and hard to maintain); software-only (not as historically accurate of the machine)

Areas: Hardware Systems, Software Systems, Circuits

Requirements

Symmetric Cryptography

- Given ciphertext and original Enigma settings, we will always produce the plaintext

Modernized Rotor Encoding

- Replace physical rotors with configurable, digital equivalent

Historical Accuracy

- Keyboard, lampboard, rotors, reflector, plugboard

Physical Dimensions

- Compact size and weight for demonstrations
- 26lbs → <5lbs

Technical Challenges

Symmetric Cryptography

- Given many encryption layers, debugging will be challenging
- **Mitigation**: verify each step before integration

Modernized Rotor Encoding

- Digitizing requires communication protocol
- Configuration must be user-controlled and durable
- **Mitigation**: backup hard-coded settings

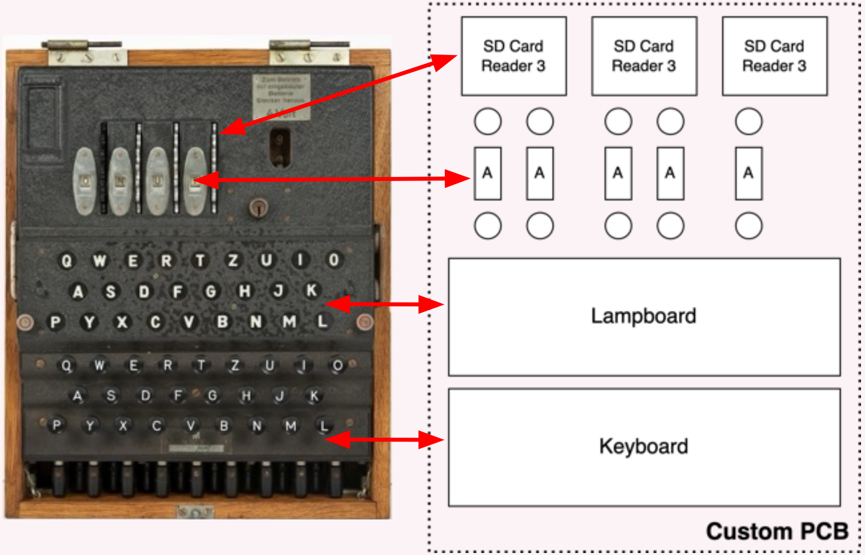
Historical Accuracy

- Balance between modernized components and maintaining historical accuracy requires considerable I/O integration

Physical Dimensions

- Electrical components need to be covered from users
- Must package Enigma in user-friendly and compact way

Solution: PCB



SD Card Reader 3

SD Card Reader 3

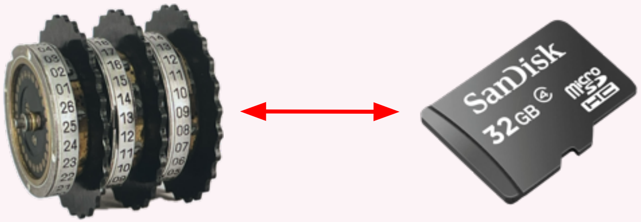
SD Card Reader 3

A A A A A

Lampboard

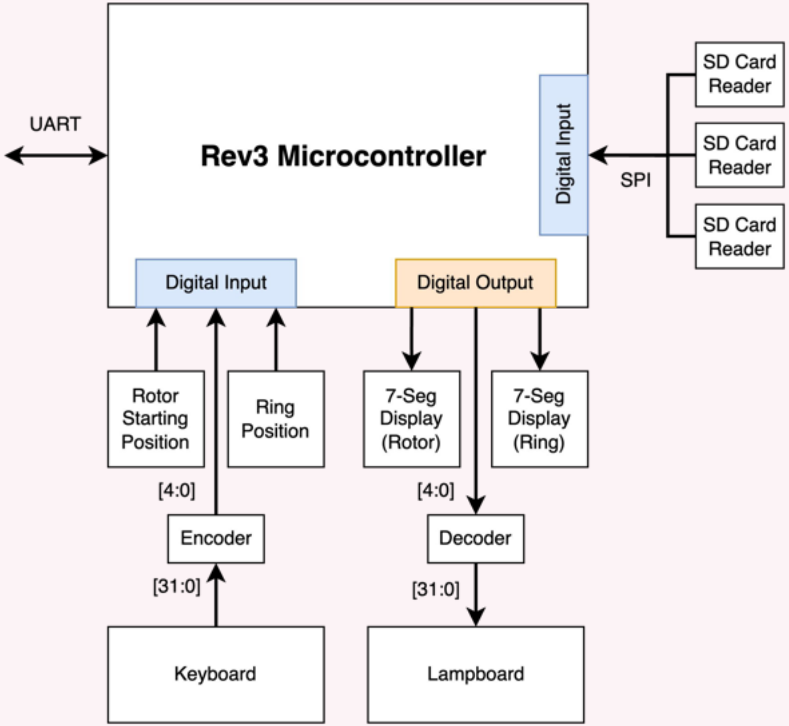
Keyboard

Custom PCB



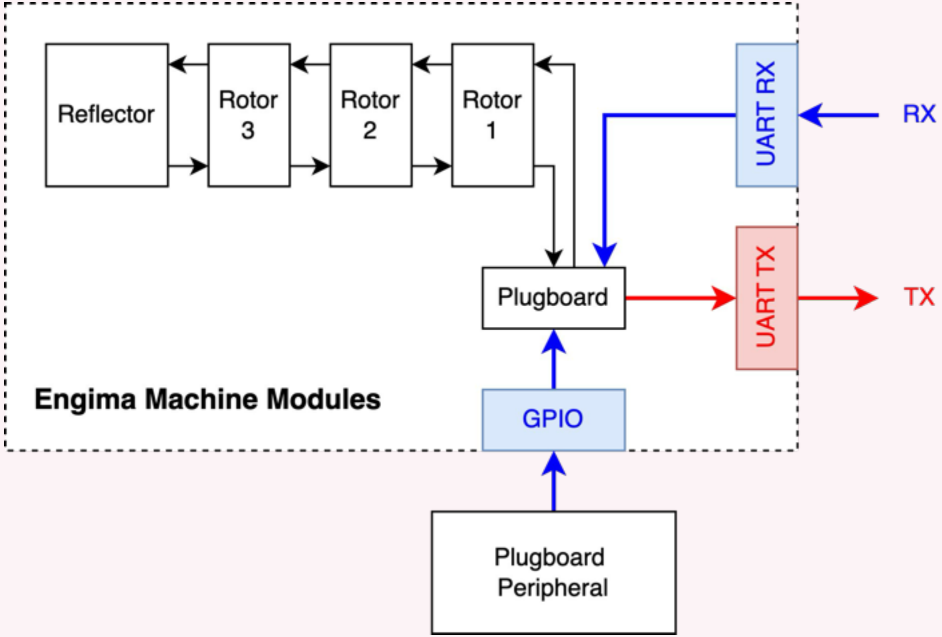
- Rotors encoded on SD cards
- Rotors and rings set with buttons
- Lampboard as LED matrix
- Keyboard as button matrix

Solution: PCB + Microcontroller



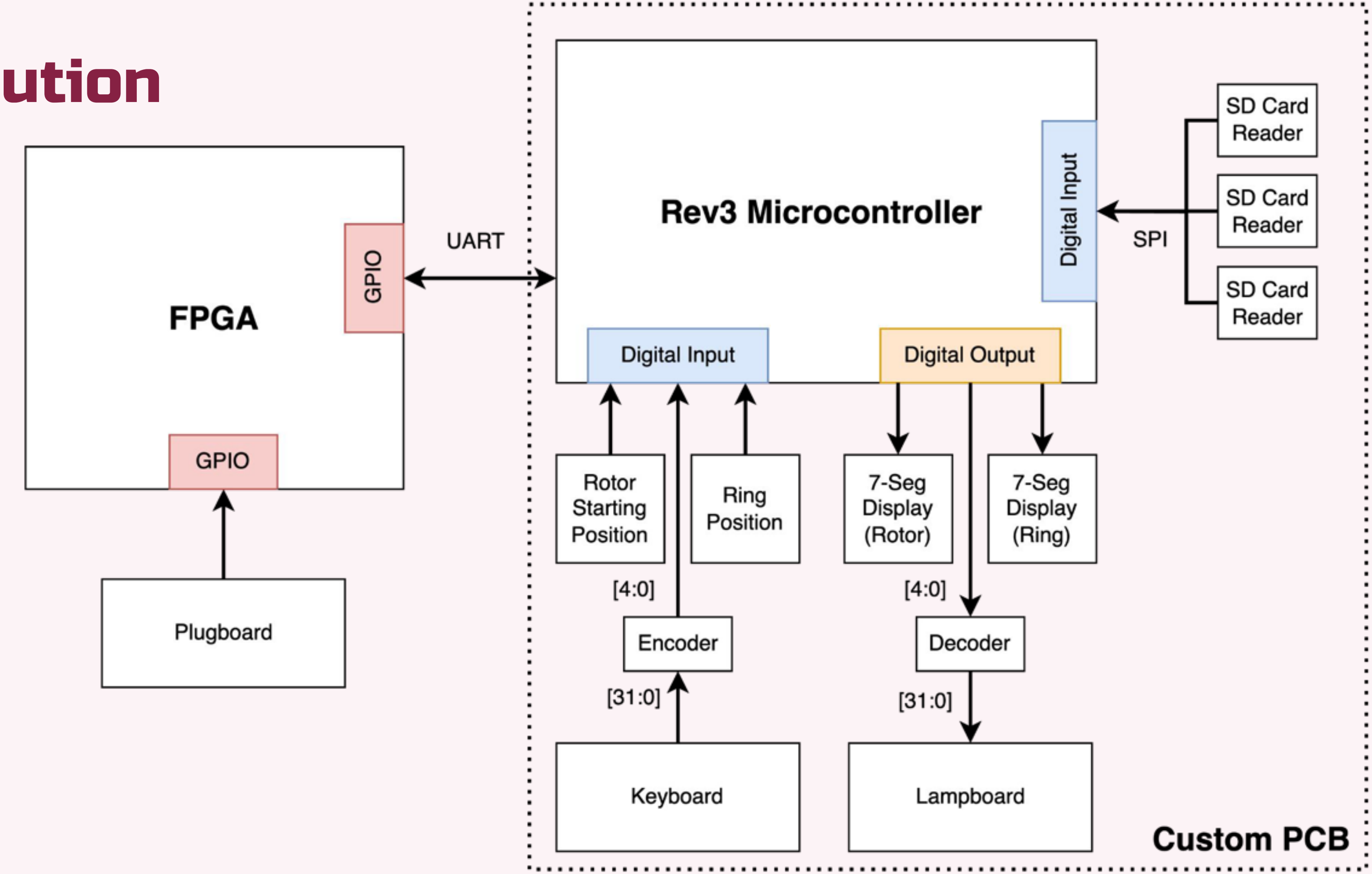
- Arduino Mega (need ~35 pins)
- SPI protocol to microcontroller
- UART protocol design
- Encoder/decoder for key/lampboard
- 7-segment display rotor/ring settings

Solution: FPGA

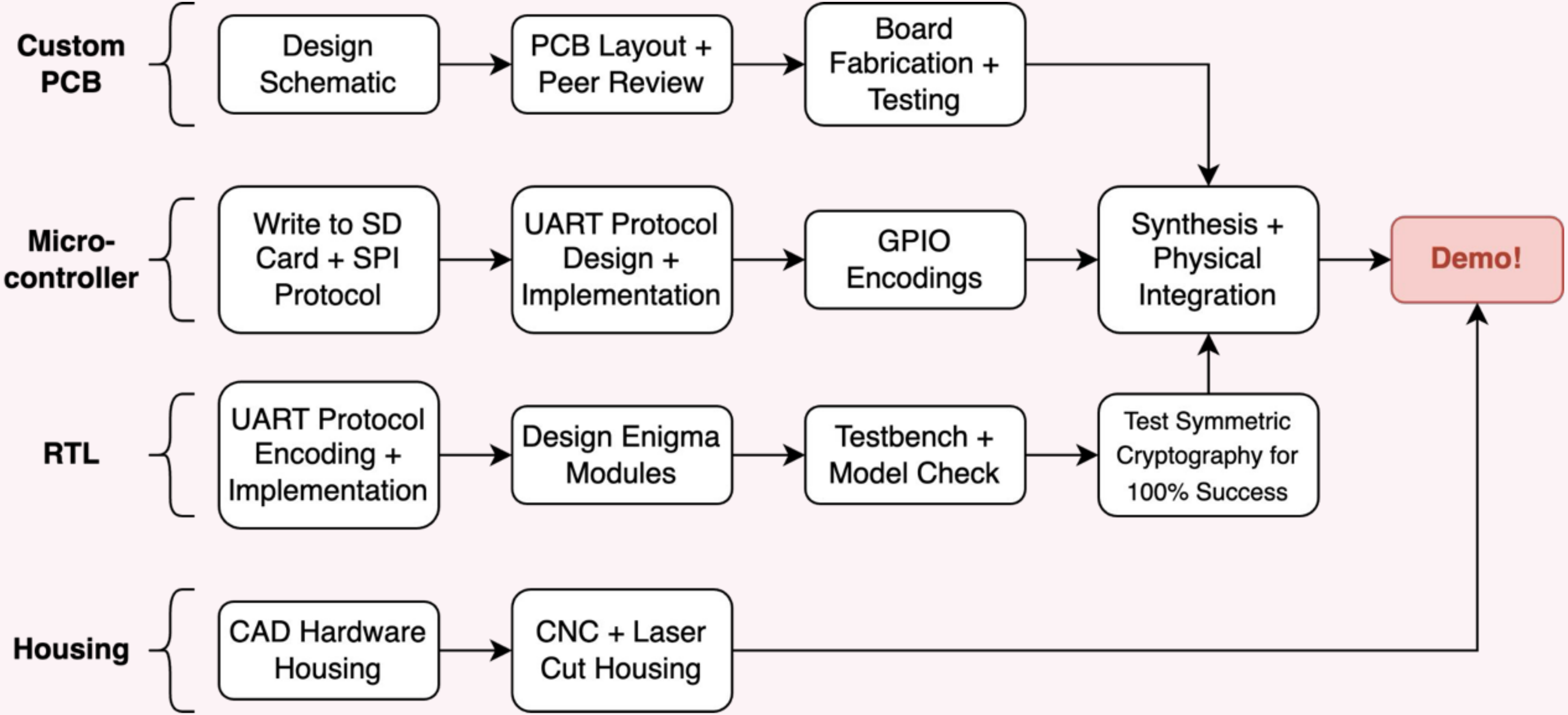


- Altera DE0-Standard Dev Board
- Replicates original hardware logic
- UART protocol design
- Rotor and reflector modules
- Plugboard interface
- Chip interface

Solution

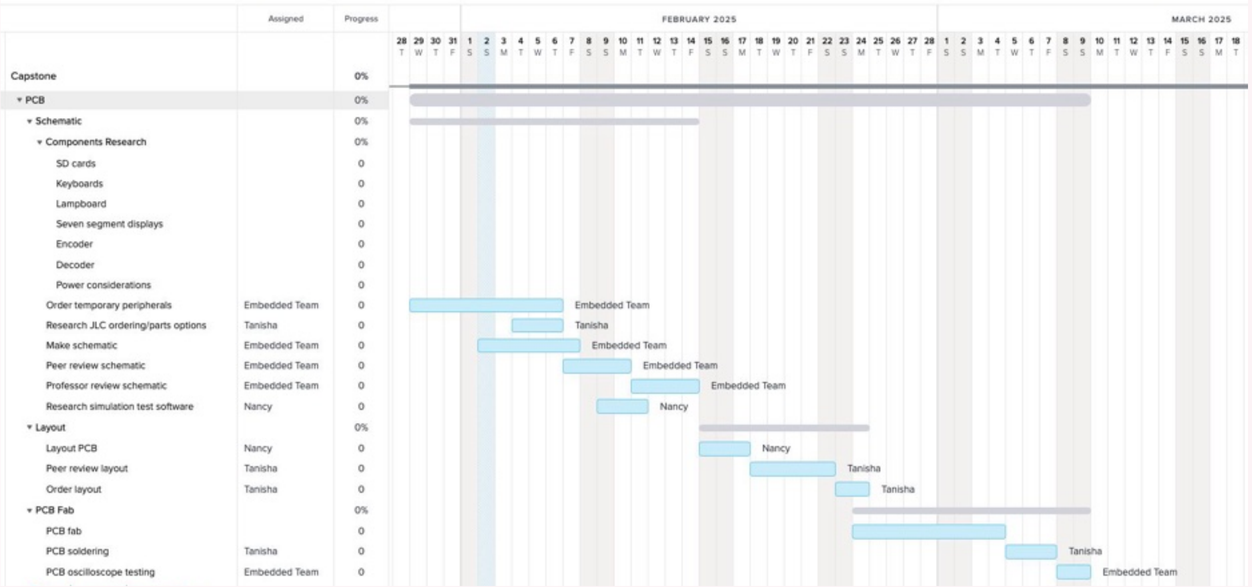

FPGA
GPIO
GPIO
Plugboard
UART
Rev3 Microcontroller
Digital Input
SPI
SD Card Reader
SD Card Reader
SD Card Reader
Digital Input
Digital Output
Rotor Starting Position
Ring Position
7-Seg Display (Rotor)
7-Seg Display (Ring)
[4:0]
[4:0]
Encoder
Decoder
[31:0]
[31:0]
Keyboard
Lampboard
Custom PCB

Testing Plan

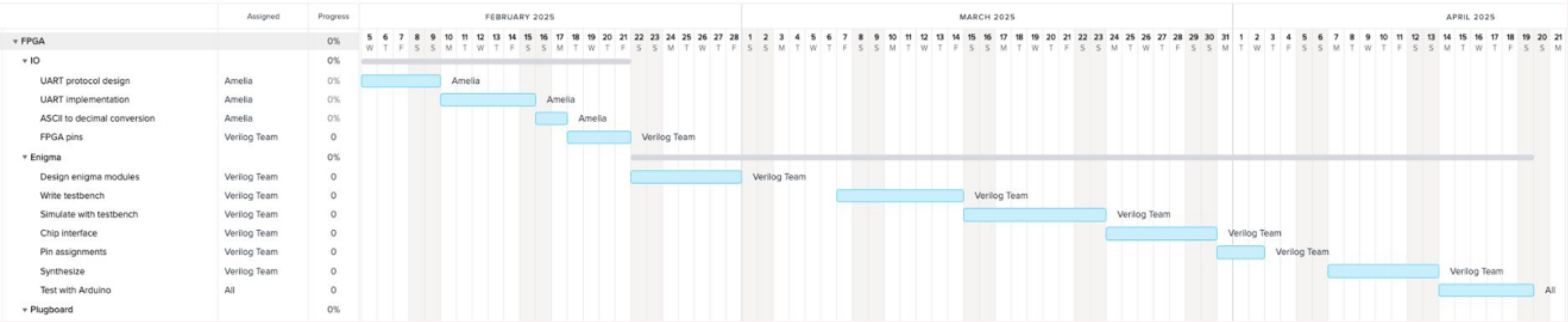

Custom PCB
Design Schematic
PCB Layout + Peer Review
Board Fabrication + Testing
Micro-controller
Write to SD Card + SPI Protocol
UART Protocol Design + Implementation
GPIO Encodings
Synthesis + Physical Integration
Demo!
RTL
UART Protocol Encoding + Implementation
Design Enigma Modules
Testbench + Model Check
Test Symmetric Cryptography for 100% Success
Housing
CAD Hardware Housing
CNC + Laser Cut Housing

Schedule + Division of Labor

Embedded Team: Tanisha + Nancy
Verilog Team: Amelia + Nancy

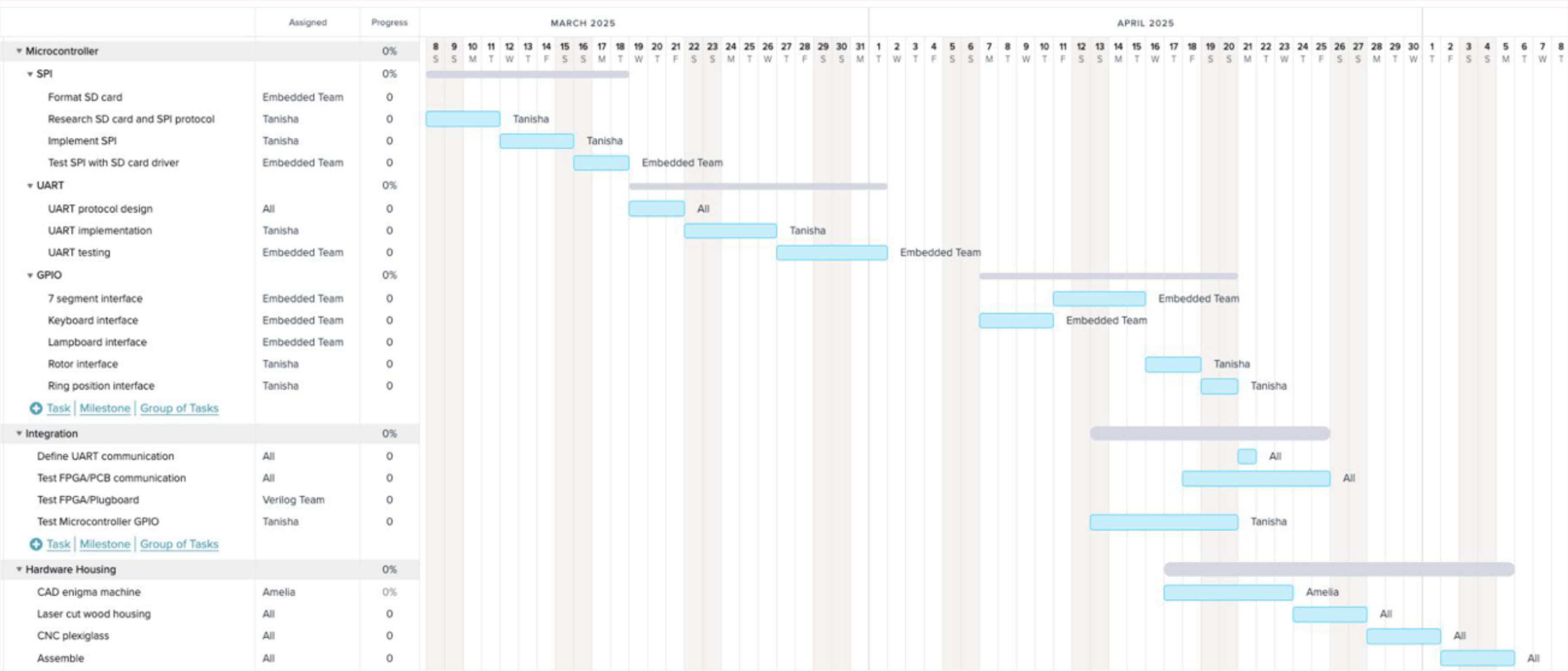


	Assigned	Progress
Capstone		0%
▾ PCB		0%
▾ Schematic		0%
▾ Components Research		0%
SD cards		0
Keyboards		0
Lampboard		0
Seven segment displays		0
Encoder		0
Decoder		0
Power considerations		0
Order temporary peripherals	Embedded Team	0
Research JLC ordering/parts options	Tanisha	0
Make schematic	Embedded Team	0
Peer review schematic	Embedded Team	0
Professor review schematic	Embedded Team	0
Research simulation test software	Nancy	0
▾ Layout		0%
Layout PCB	Nancy	0
Peer review layout	Tanisha	0
Order layout	Tanisha	0
▾ PCB Fab		0%
PCB fab		0
PCB soldering	Tanisha	0
PCB oscilloscope testing	Embedded Team	0



	Assigned	Progress
▾ FPGA		0%
▾ IO		0%
UART protocol design	Amelia	0%
UART implementation	Amelia	0%
ASCII to decimal conversion	Amelia	0%
FPGA pins	Verilog Team	0
▾ Enigma		0%
Design enigma modules	Verilog Team	0
Write testbench	Verilog Team	0
Simulate with testbench	Verilog Team	0
Chip interface	Verilog Team	0
Pin assignments	Verilog Team	0
Synthesize	Verilog Team	0
Test with Arduino	All	0
▾ Plugboard		0%

Schedule + Division of Labor



	Assigned	Progress
▾ Microcontroller		0%
▾ SPI		0%
Format SD card	Embedded Team	0
Research SD card and SPI protocol	Tanisha	0
Implement SPI	Tanisha	0
Test SPI with SD card driver	Embedded Team	0
▾ UART		0%
UART protocol design	All	0
UART implementation	Tanisha	0
UART testing	Embedded Team	0
▾ GPIO		0%
7 segment interface	Embedded Team	0
Keyboard interface	Embedded Team	0
Lampboard interface	Embedded Team	0
Rotor interface	Tanisha	0
Ring position interface	Tanisha	0
Task | Milestone | Group of Tasks		
▾ Integration		0%
Define UART communication	All	0
Test FPGA/PCB communication	All	0
Test FPGA/Plugboard	Verilog Team	0
Test Microcontroller GPIO	Tanisha	0
Task | Milestone | Group of Tasks		
▾ Hardware Housing		0%
CAD enigma machine	Amelia	0%
Laser cut wood housing	All	0
CNC plexiglass	All	0
Assemble	All	0

MARCH 2025
APRIL 2025
8 S 9 S 10 M 11 T 12 W 13 T 14 F 15 S 16 S 17 M 18 T 19 W 20 T 21 F 22 S 23 S 24 M 25 T 26 W 27 T 28 F 29 S 30 S 31 M
1 T 2 W 3 T 4 F 5 S 6 S 7 M 8 T 9 W 10 T 11 F 12 S 13 S 14 M 15 T 16 W 17 T 18 F 19 S 20 S 21 M 22 T 23 W 24 T 25 F 26 S 27 S 28 M 29 T 30 W
1 T 2 F 3 S 4 S 5 M 6 T 7 W 8 T
Tanisha
Tanisha
Embedded Team
All
Tanisha
Embedded Team
Embedded Team
Embedded Team
Tanisha
Tanisha
All
All
Tanisha
Amelia
All
All
All

A riddle wrapped in a mystery inside an *enigma* !

- Modernized implementation of the WWII Enigma machine
- Lightweight, durable, reconfigurable, while staying true to historical look
- Hands-on education in museums + classrooms
- FPGA + custom PCB + microcontroller

Q W E R T Z U I O
It's the greatest encryption device in history.
The Germans use it for all major communications.