B5: ENIGMA18

Nancy Anderson
Amelia Lobo
Tanisha Sethi

APPLICATION

- Modernized implementation of WWII Enigma machine

USE CASE

- Educate about **historical cryptography** through hands-on encryption and decryption
- For use in museums and classrooms (**open-source**)

EXISTING SOLUTIONS

- Electromechanical (historical), software-emulators (not historically accurate)

Viewing of CMU's 3-rotor Enigma machine, Courtesy of Sam Lemley, Curator of Special Collections at CMU Libraries

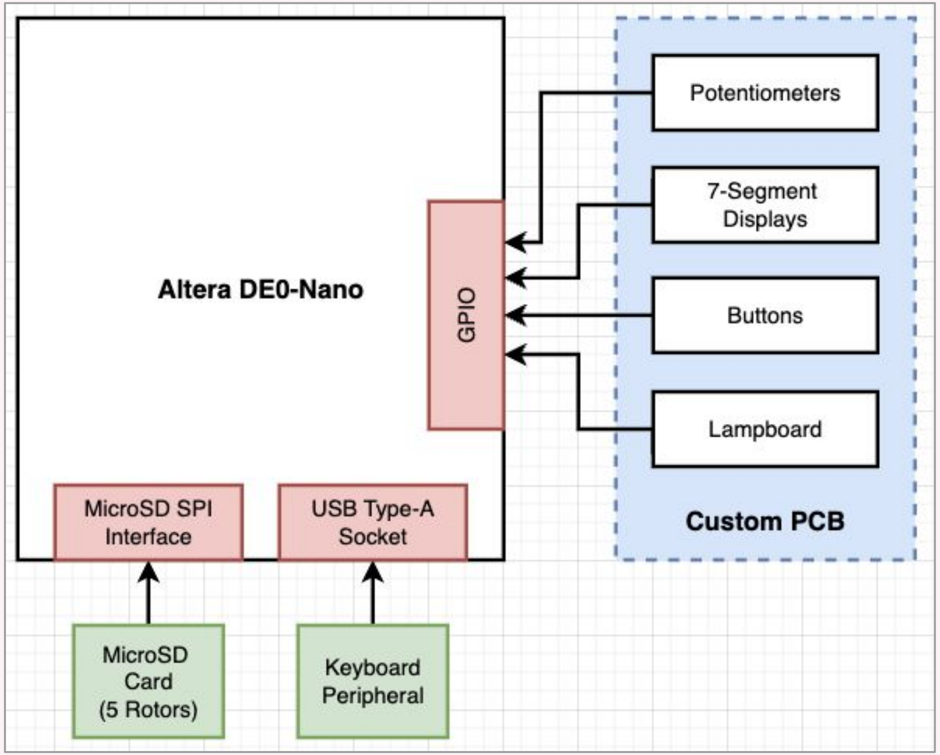
Quantitative Use-Case Requirements

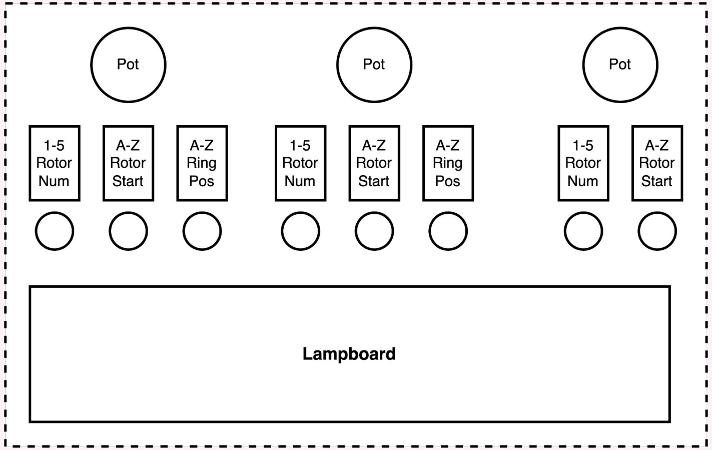
USE-CASE	DESIGN REQUIREMENT
I/O to represent all **26** letters of alphabet	• **26** LEDs and **26** keys
Compact size to be **held in two hands**	• Fit on DE0-Nano (**49mm x 75.2 mm**) header pins
Must have **1,054,560** combinations (number of configs for 3-rotor machine) Rotor (Pick 3 of 5 Rotors): $\frac{5!}{(5-3)!}$ ways Starting Config (1 of 26 for 3 rotors): $26^3 = 17,576$ ways Total Combinations: $60 * 17,576 = 1,054,560$ ways	• Configurable rotors (pick **3 of 5**) • Configurable rotor starting position (**26**) • Configurable ring position

Quantitative Use-Case Requirements

USE-CASE	DESIGN REQUIREMENT
Hold complete encodings of **5** rotors on peripheral storage unit (configurability)	• Peripheral storage unit should hold **130B** of information (**5 * 26B**)
Simulate "instantaneous" rotor rotation under human reaction time of **250ms**	• FPGA must **read 130B in <= 250ms** • SPI bandwidth **> 4.16 Kbps**
Power consumption only requires **1 standard wall outlet**	• FPGA **5V** mini-USB wall adapter • LEDs & 7-seg displays operate at **3.3V** from GPIO pins
100% of computation and interfacing should be done on FPGA	• Must use **<= 70 GPIO pins** (not including GND, 3.3V, 5V)

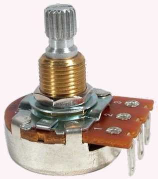
System Specification

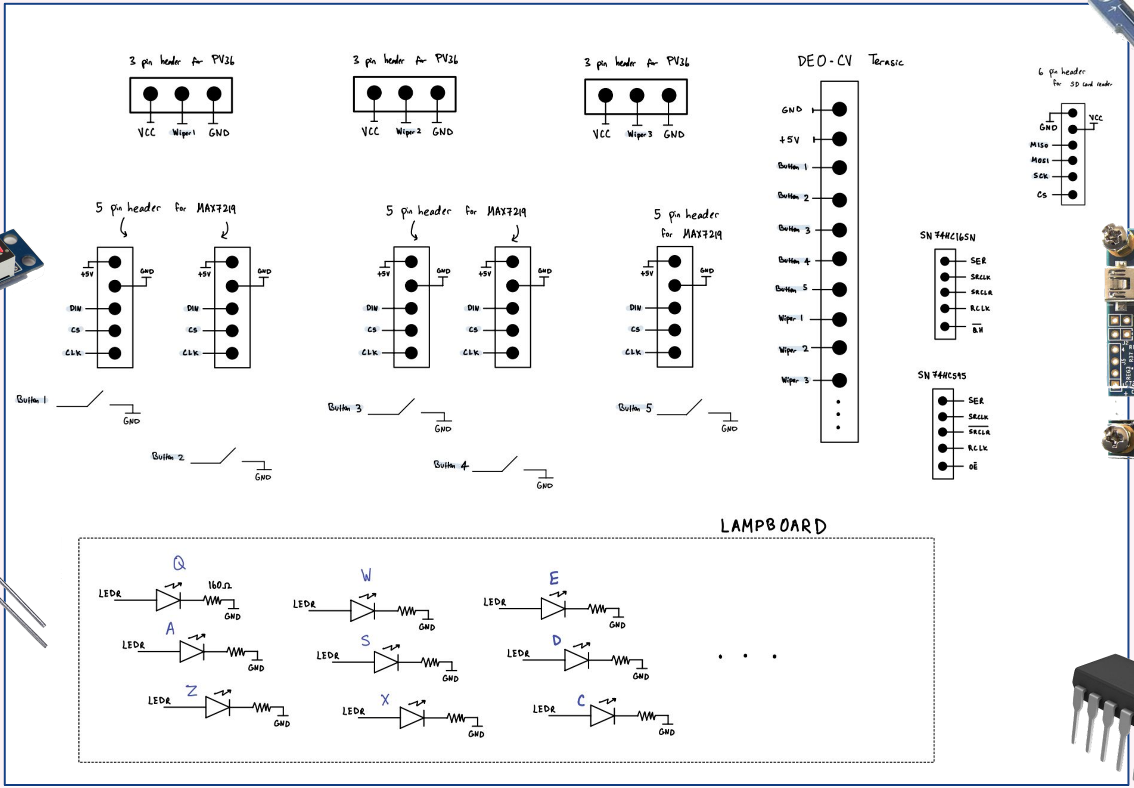


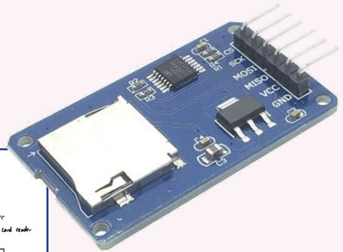


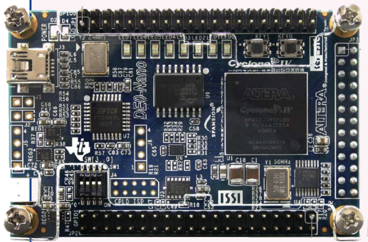
- **Potentiometer (3):** Handles setting rotor number, rotor starting, ring position via FPGA ADC pins
- **7-segment display (8):** Display Enigma settings
- **Button (8):** Change Enigma settings
- **LED matrix (26):** Lampboard

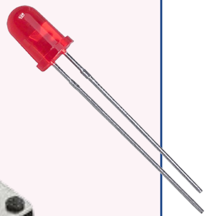
Implementation Plan: PCB Schematic

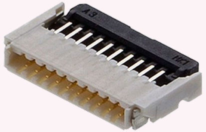


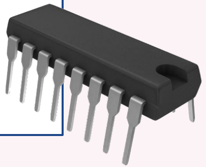








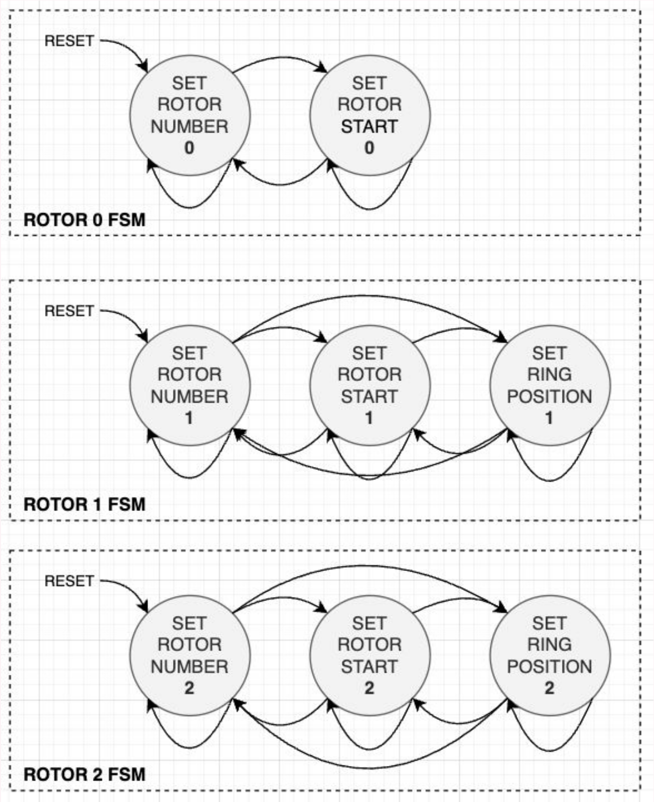


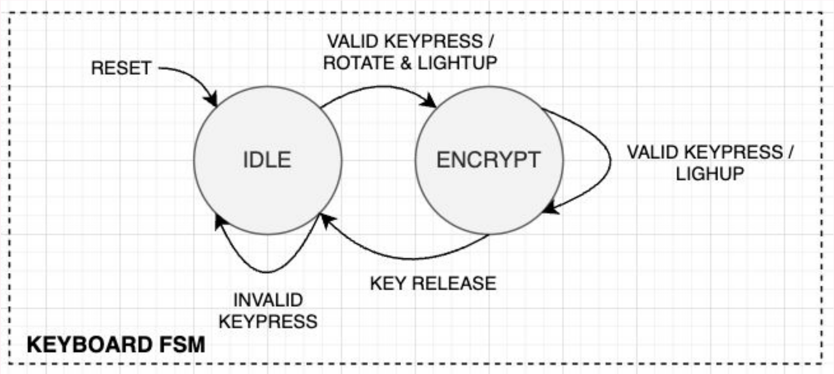


Implementation Plan: PCB Tradeoffs

CHOSEN	CONSIDERED	JUSTIFICATION
Shift Registers	Multiplexers	Optimized FPGA pin usage (70 pins) to reduce hardware complexity
MAX7219 7-Segment Display	LCD Display	Use of SPI protocol (only 3 pins) for efficient communication with **low power consumption**
Single SD Card	3 SD Card Readers	**Historical accuracy** for customisable encodings Streamlined **user experience** by reducing unnecessary hardware
External Keyboard	Custom PCB Keyboard	Enhanced **accessibility** with a **safer**, user-friendly interface (reduced exposure to live PCB components)
Panel-mount rotary potentiometer	Rotary shift potentiometer	Smoother analog input for precise control to improve reading **accuracy**

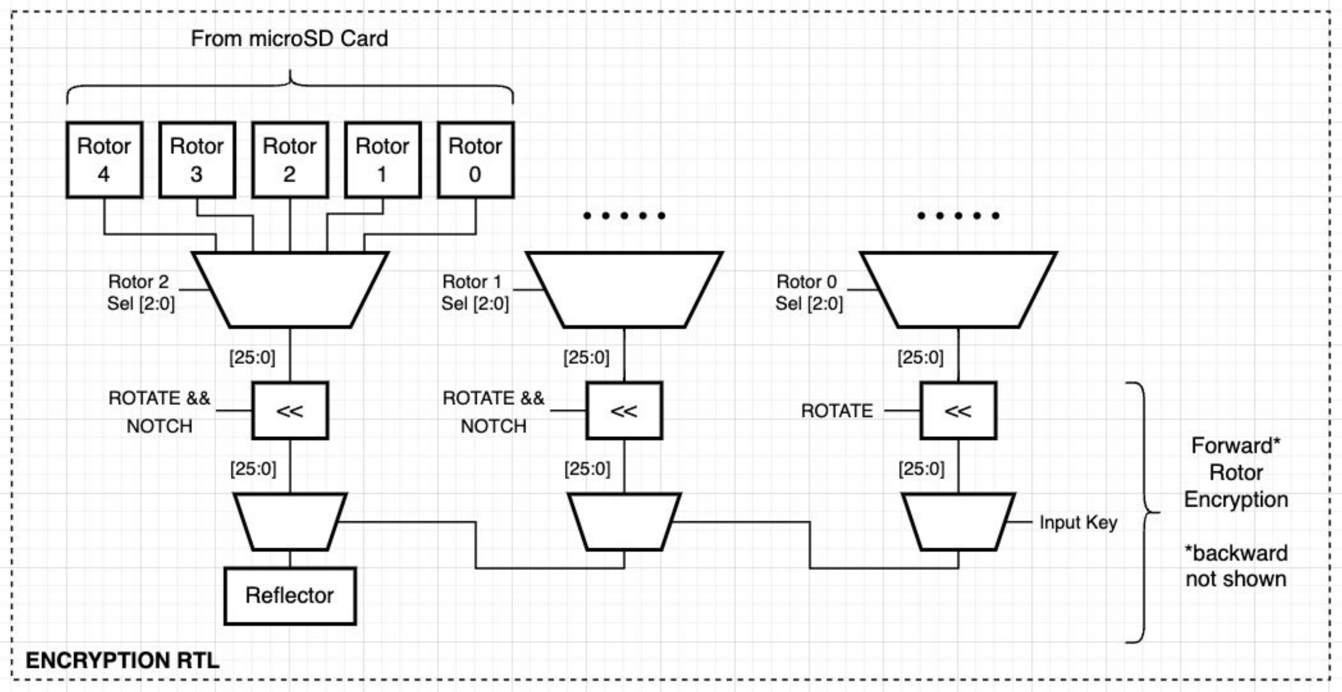
Implementation Plan: FSMs





- **Rotor 0-2 FSMs**
  - Handles rotor setting inputs from buttons and potentiometer
  - Handles updates to 7-segment output
- **Keyboard FSM**
  - Rotates rotors and encrypts plaintext to ciphertext on keypress

Implementation Plan: RTL



- Input key from keyboard
- Read microSD card via SPI
- Select rotors, starting settings, and ring settings through PCB
- Reverse encryption though reflector module

Testing, Verification, Validation

AREA	TEST METHOD	DESIGN REQUIREMENT
PCB	Design Rule Check	Verify design meets manufacturing requirements with **0 errors**
	Electrical Rule Check	Verify power and ground connections with **0 errors**
	Multimeter	**Continuity test**, ensure proper fabrication with **0 open circuits**
Peripherals	H2TestW for microSD	**10** tests show **0% data corruption** on **130B** of rotor encodings
RTL Synthesis	Peripheral unit testing	• Lampboard: Lights up random sequence of **50 letters** • MicroSD: Read and write **10 times** with different rotor encodings • Keyboard: Type for **2 minutes**, ensure all letters accurate
	Integrative user testing	• Test Enigma machine on **5 people**, have them change each rotor number, rotor setting, and ring setting

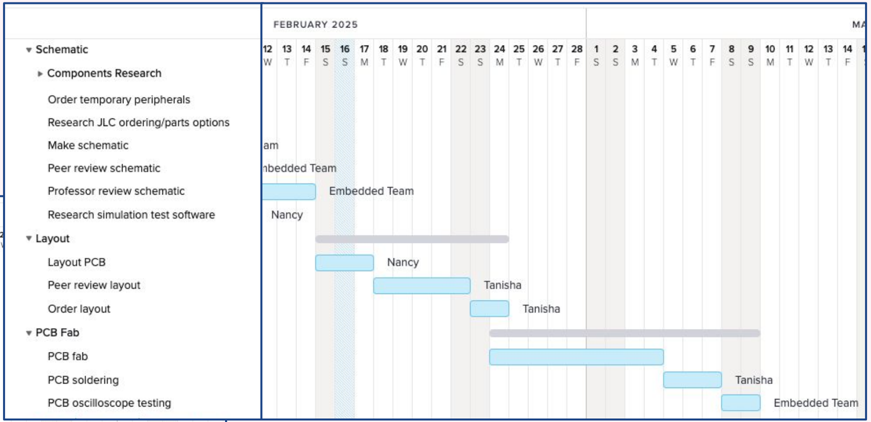
Testing, Verification, Validation

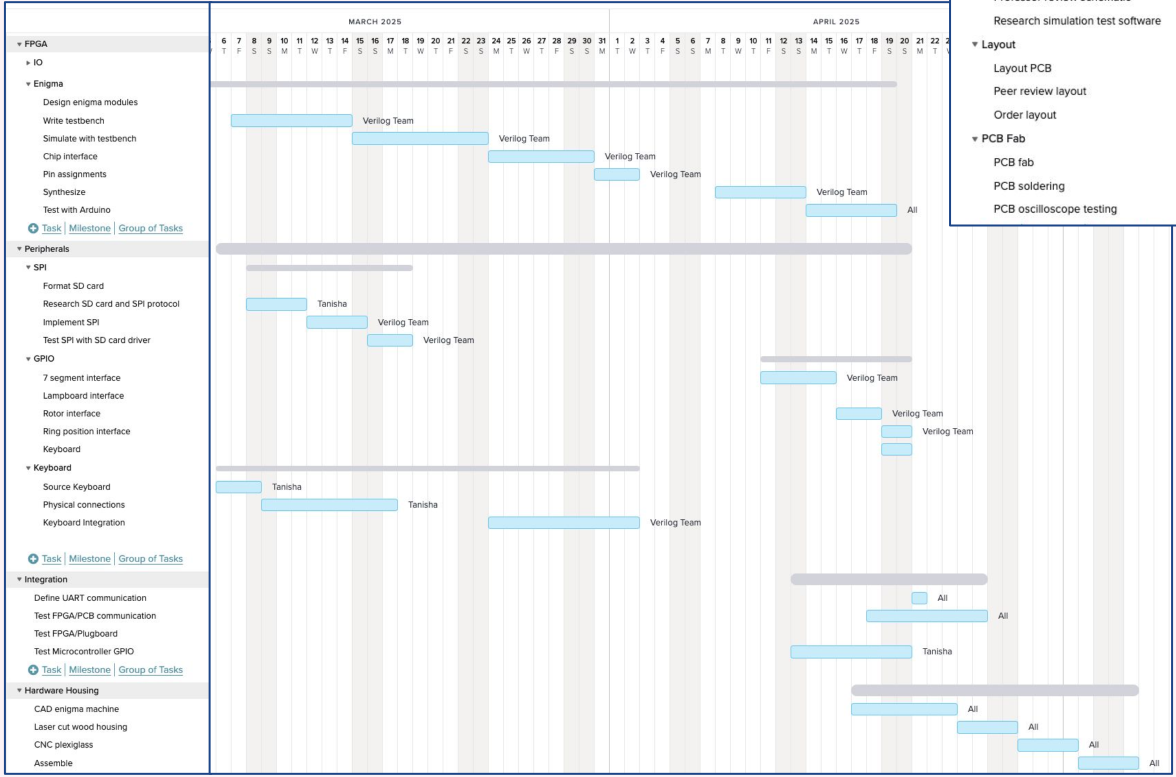
AREA	METHOD	DESIGN REQUIREMENT
RTL Simulation	Constrained Random Tests	Rotor logic **100% accuracy**: Input **500** randomized plaintext characters → ciphertext → plaintext **20** randomized Enigma settings
		MicroSD: **20** randomized **130B** sequences with SPI protocol
		Keyboard: **20** randomized **200** inputs with matrix scanner algorithm
	Directed Testing	Corner cases and general cases
	Model Checking	Immediate and concurrent assertions

Testing, Verification, Validation

RISK	MITIGATION
Faulty PCB fabrication	• Unit test with breadboard components
FPGA ADC pins do not have sufficient resolution for 26 letters	• SMD potentiometer (vs through-hole) • Alternatively use buttons alone to encode rotor information
Unable to read from microSD card into FPGA	• Hardcoded RTL rotor encodings • Rotors can still be selected via buttons
Keyboard matrix scanner algorithm fails	• Alternatively can use the USB OTG on the FPGA to interface with a USB peripheral keyboard

Project Management





EMBEDDED TEAM :
Tanisha + Nancy

VERILOG TEAM :
Amelia + Nancy