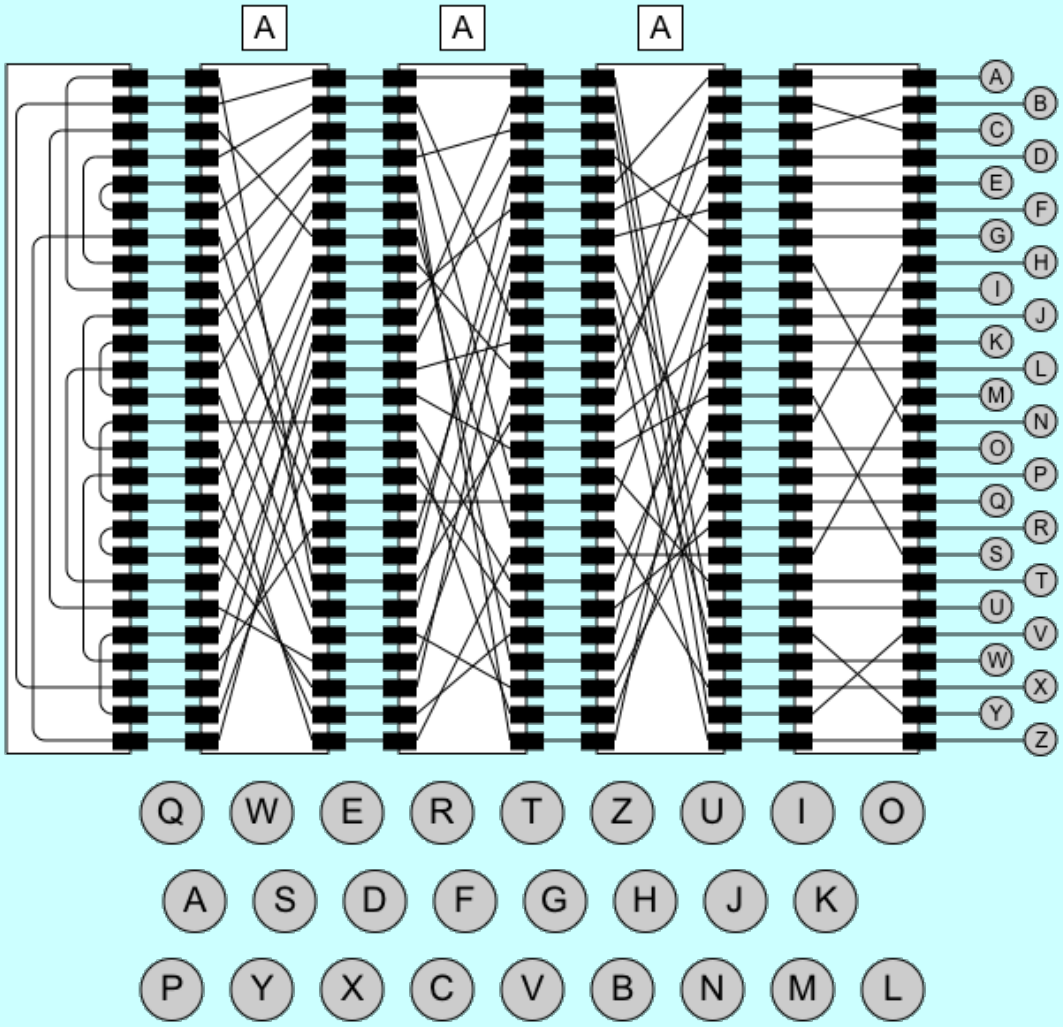
The Enigma Machine

Jerry Cain
CS 106AX
October 23, 2023

slides constructed from images created by Eric Roberts for his Enigma Machine assignment

The Enigma Machine

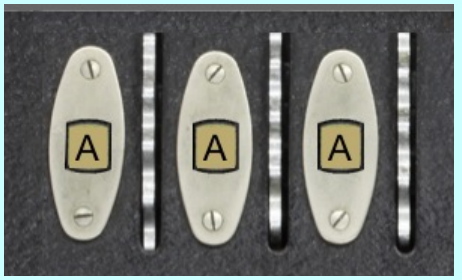


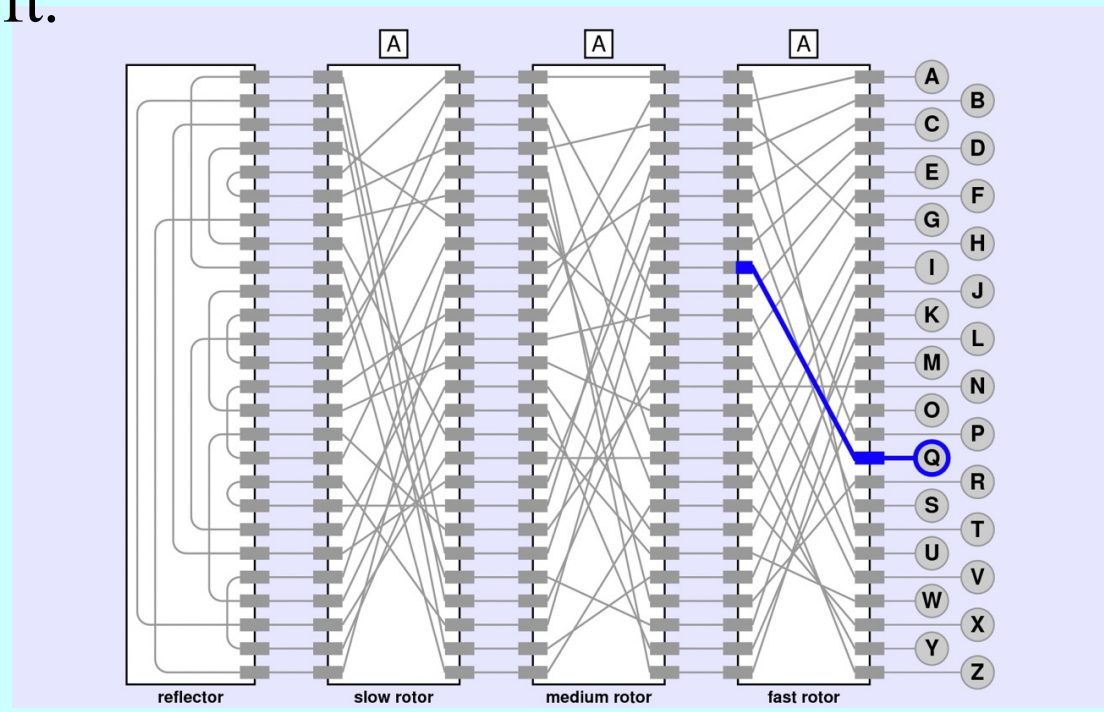
Enigma Machine in CS106AX

- Assignment 4 has you simulate the Enigma machine used by the German military during much of World War II.
- Your simulation implements an aerial view of an Enigma machine like that presented below.
- The rotors along the top dictate how several letter-substitution ciphers are chained together to encrypt a single key press.
- The physical keys occupy the lower third of the machine. Each key press triggers an electrical impulse through the rotors and back to illuminate one of 26 lamps, which occupy the middle portion of the machine.

Enigma Machine Rotors

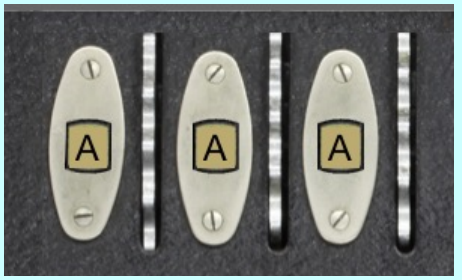
- The three rotors collectively operate as a base-26 odometer. The rotors themselves allow current to pass from each of 26 connections on the right to one of 26 connections on the left.
- In the AAA configuration, the Q on the fast rotor's right is wired to the I on the fast rotor's left.
- Similarly, the A on the right maps to the B on the left, B maps D, etc.

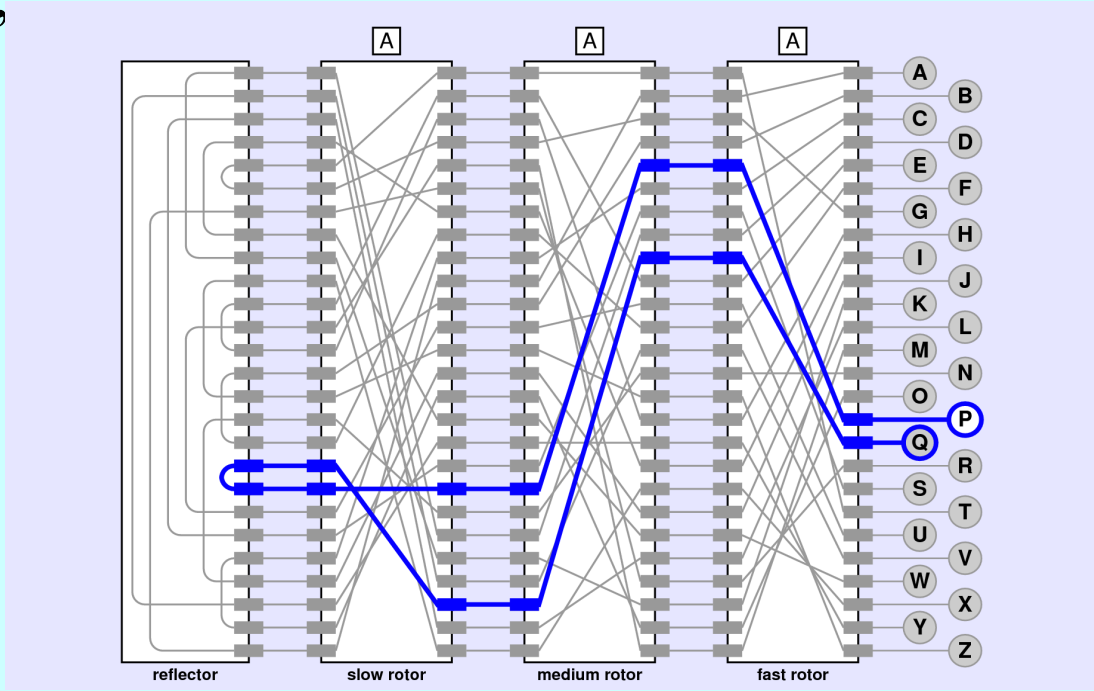




Enigma Machine Rotors

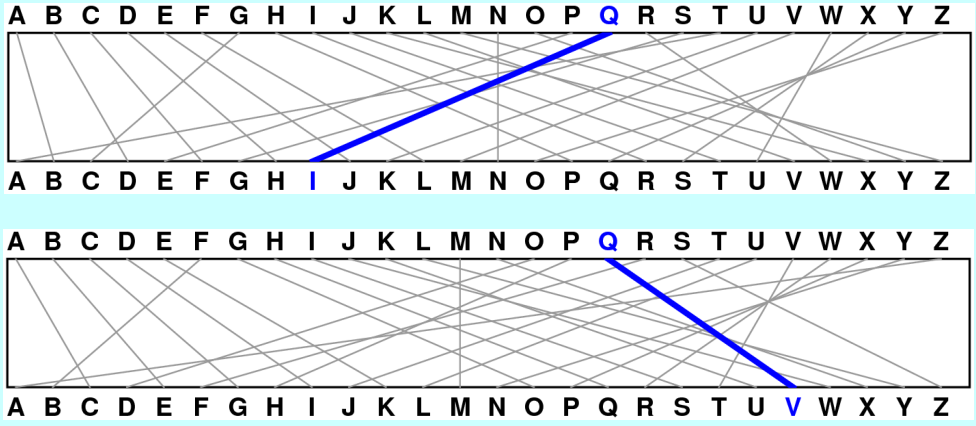
- As electrical current passes from right to left, the output of the fast rotor lines up with some input on the medium rotor, which provides its own letter-substitution cipher.
- In the AAA configuration, the medium rotor maps the I position to the A position, and the slow rotor maps the X on its right to the R own its left.
- The leftmost component is the reflector, which connect input pairs so current reverses direction and passes back through the three rotors to a lamp.





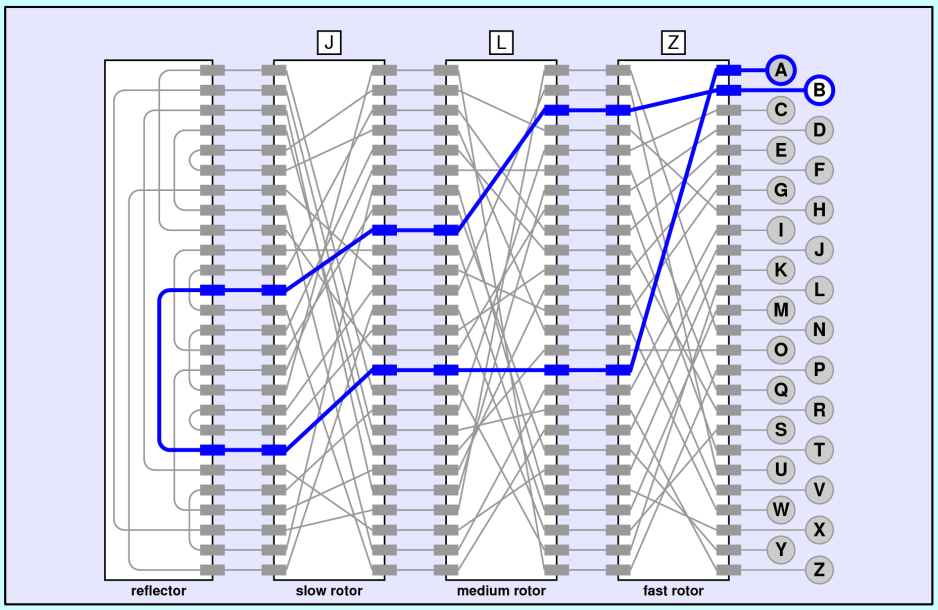
Enigma Machine Rotors

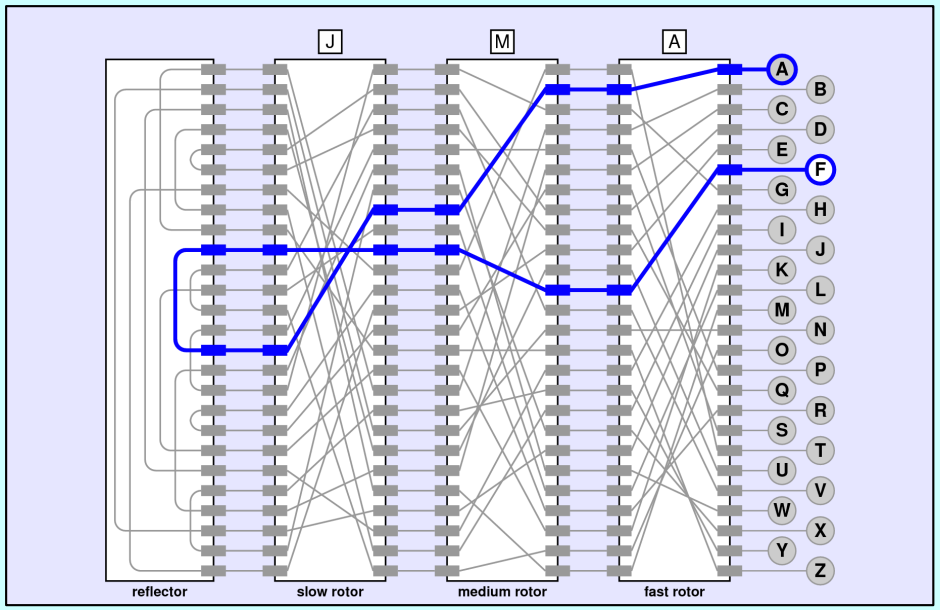
- When discussing how a rotor encodes a particular input, one can articulate the encoding in two different ways:
  - The physical key for the letter Q is wired to an input on the right that represents the letter I on the left, or
  - The physical key for the letter Q is wired to an input on the right that encrypts the Q by **rewinding it** eight positions in the alphabet.
- The second articulation is more useful than the first, because the rewind (and advance) rhetoric generalizes more easily as the rotor itself advances.
- If the fast rotor advances one notch, the wire that previous advanced R five positions now advances Q five positions.



Enigma Machine Rotors

- To understand how the encryption evolves, look at the encryption in the below left figure, noting that A becomes P becomes P becomes T becomes L (via reflection) becomes I becomes C becomes B.
- Also notice that B on the fast rotor's right maps to C on that rotor's left. On the next key press, that connection will rotate so the connection that once led B to C now connects A to B, as it does in the lower right figure.





The End