Eric Roberts and Jerry Cain
CS 106J

Handout #36
May 15, 2017

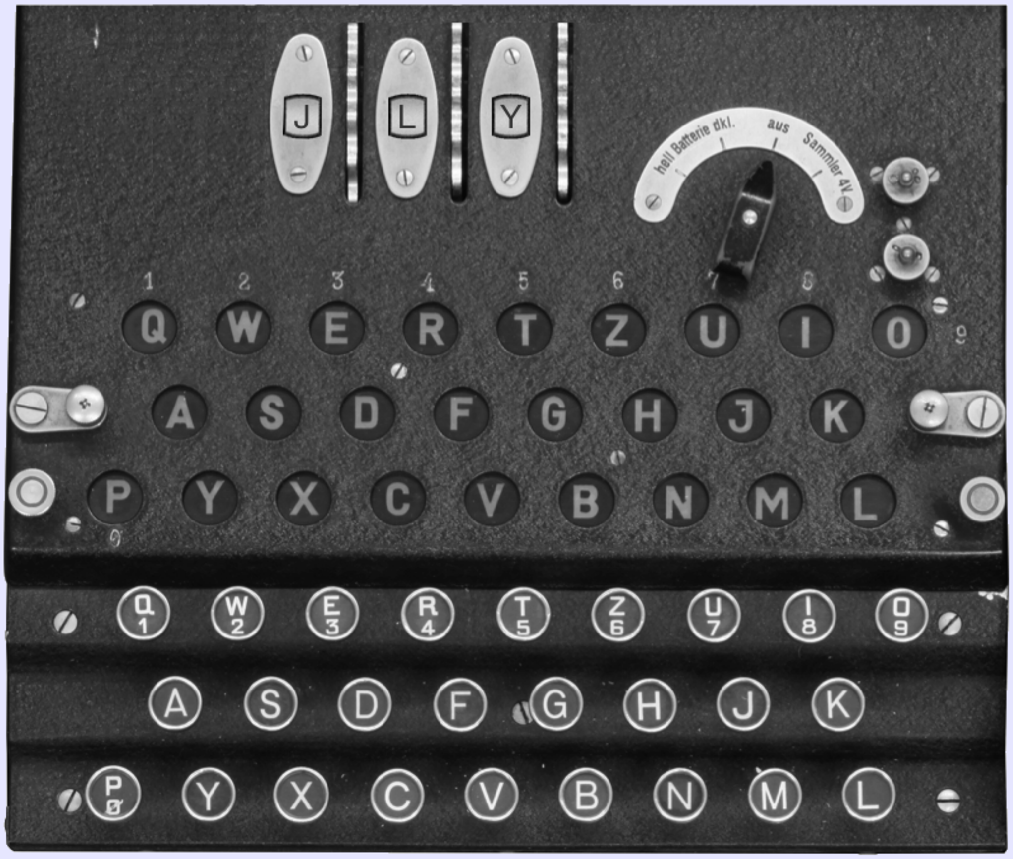
The Enigma Machine

In World War II, a team of British mathematicians working at a secret facility called Bletchley Park was able to break the German military code, which allowed the Allies to decipher German military communication. Breaking the German codes was an early application of ***cryptography,*** which is the science of creating and decoding messages. In the language of cryptography, the message you want to send is called the ***plaintext;*** the encoded message is called the ***ciphertext.*** Decoding the ciphertext typically depends on having the sender and receiver share a privileged piece of information called a ***key.***

In the early 1930s, the German military adopted a new encryption protocol based on an existing commercial device called ***Enigma.*** This handout describes the operation of the Enigma machine in enough detail for you to simulate its function in Assignment #5. A detailed account of how the Bletchley Park mathematicians broke Enigma is available on the CS 106J website.

Figure 1 shows the top view of a typical Enigma machine, expanded so that you can see the detail. At the bottom of the figure is a keyboard arranged in the standard German

Figure 1. Top view of a typical Enigma machine



layout. Above the keyboard are three rows of lamps. Pressing a key lights one of the lamps, thereby indicating the encoded version of that letter. The mapping from keys to lamps is controlled by the three thumb wheels at the top of the diagram, which are called ***rotors.*** Each rotor—which in the wartime Enigma machines could be chosen from a stock of five rotors from which any three could be used in any order—can be set to any of 26 positions corresponding to the letters of the alphabet. The display windows at the top of Figure 1 show the letters **JLY**. The three letters together are called the ***rotor setting.***

Enigma rotors are three-dimensional, which unfortunately makes them difficult to represent on the printed page. The letters you see through the display windows are printed around the circumference of the rotor. The left and right edges of a rotor have 26 electrical contacts aligned with the 26 letters. Those contacts are wired across the rotor so that each contact on the left connects to a contact on the right in some scrambled arrangement. Each rotor therefore implements a reordering of the letters of the alphabet, which mathematicians call a ***permutation.***

Figure 2 offers two views of this wiring. The diagram on the left shows how the rotor would appear when viewed along its axis. The letters circle the rotor, and the contacts shown at the outer edge go through the rotor and connect to the contact in the interior circle, which are physically on the opposite side of the rotor itself. The contact **A** on this side of the rotor connects to contact **E** on the reverse side, as shown by the heavy line in the diagram. The diagram on the right offers a schematic view in which the connections across the rotor appear in a linear arrangement. This diagram has the same wiring, as indicated by the connection between **A** on the right and **E** on the left. When you look at this "unrolled" view, you have to keep in mind that the top and bottom of the rectangle are in fact connected together to form a circle.

Figure 2. Two views of the wiring of an Enigma rotor

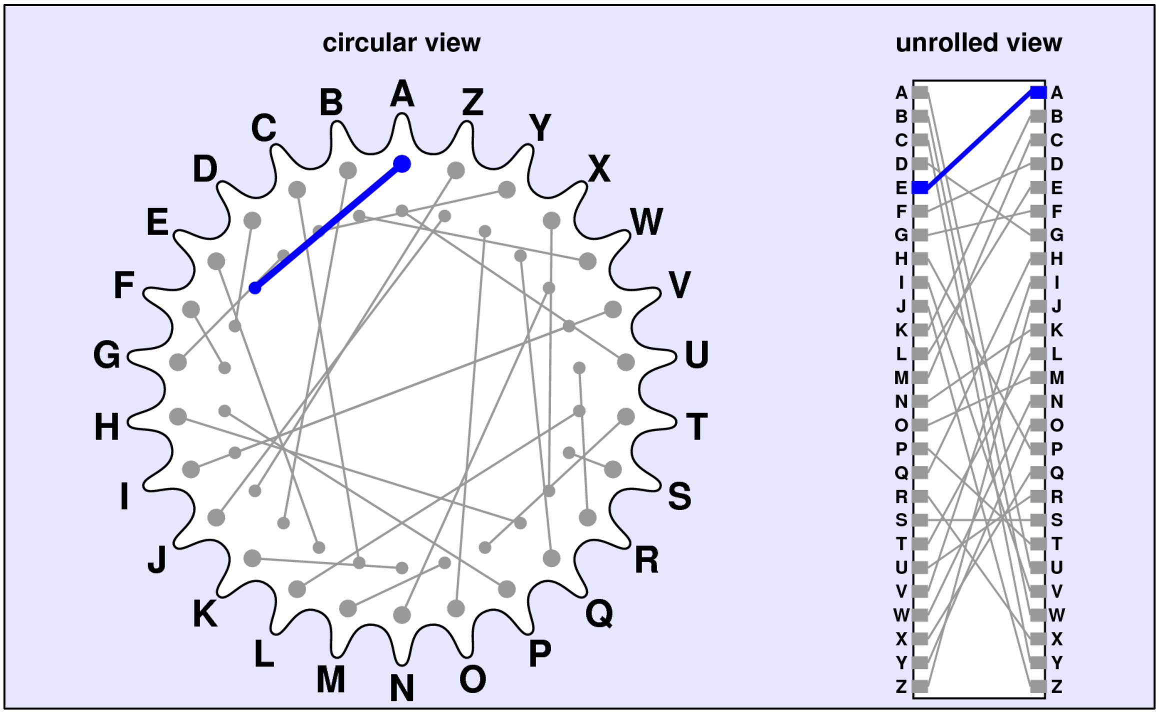

circular view
A
Z
Y
X
W
V
U
T
S
R
Q
P
O
N
M
L
K
J
I
H
G
F
E
D
C
B
unrolled view
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Figure 3 shows the internal structure of the Enigma machine, focusing on how the wiring of the three rotors makes it possible to encrypt information as it passes from one side of the machine to the other. Typing a character on the keyboard automatically advances the rotor on the right, thereby changing the pattern of connections inside the machine. When the rightmost rotor has completed a full revolution, the middle rotor advances one step; in much the same way, completing a revolution of the middle rotor advances the leftmost rotor. The rotors therefore advance in a fashion reminiscent of the odometer on a car. The right rotor advances on every character and is therefore called the ***fast rotor.*** The middle rotor advances once every 26 characters and is called the ***medium rotor.*** The left rotor advances only once every 676 (26 × 26) characters and is called the ***slow rotor.***

Figure 4 at the top of the next page shows what happens if the operator types the **A** key. Pressing the key advances the fast rotor, which changes the rotor setting from **JLY** to **JLZ**. The Enigma machine then applies a current to the wire leading from the **A** key at the right edge of the diagram and, at the same time, disconnects the **A** lamp so that only the encrypted version of the letter appears. The current flows from the **A** key through each of the three rotors, moving from right to left. It then passes into a circuit element called the ***reflector,*** which implements a fixed permutation. From the reflector, the current flows back across the rotors in the opposite direction. As shown in the diagram, the current initiated by typing **A** ends up on the wire labeled **B**, which causes the **B** lamp to light. Thus, given the rotor setting **JLZ**, the ciphertext form of the letter **A** is **B**.

The encryption patterns generated by the Enigma machine are difficult to break because the encoding changes on every character. If the operator types a second letter **A** immediately after the first, the fast rotor again advances, which this time completes the

Figure 3. Structural diagram of the Enigma machine showing the rotor setting JLY

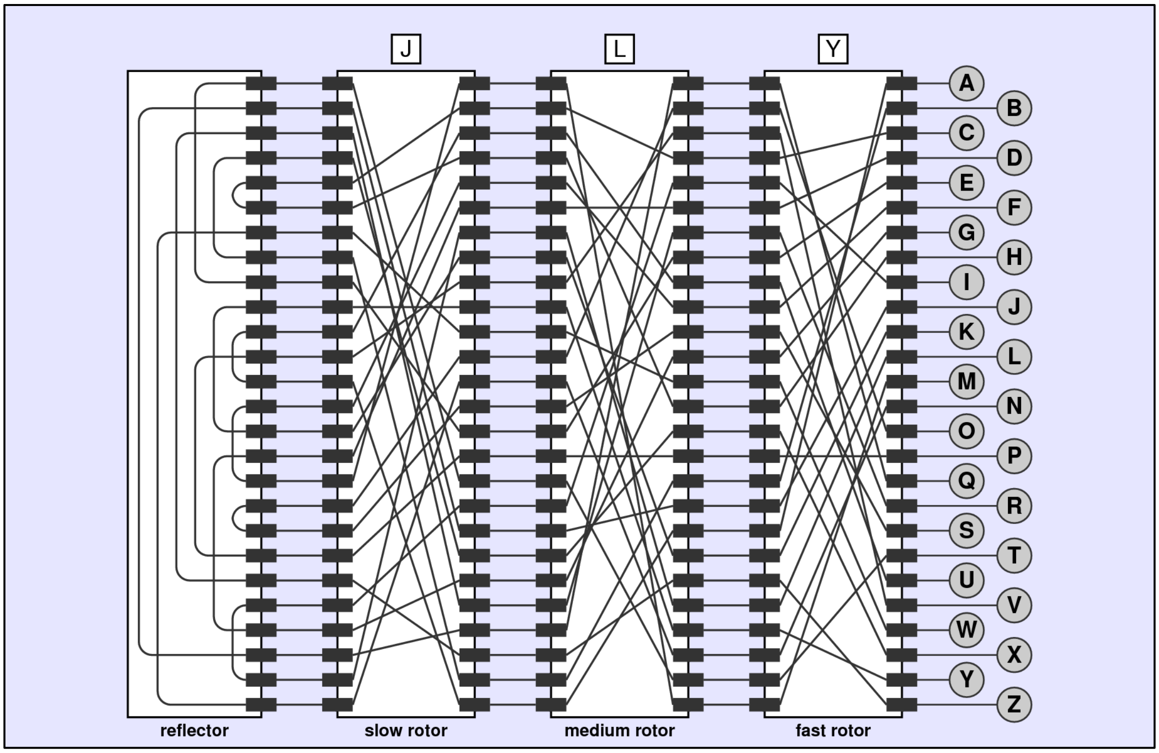
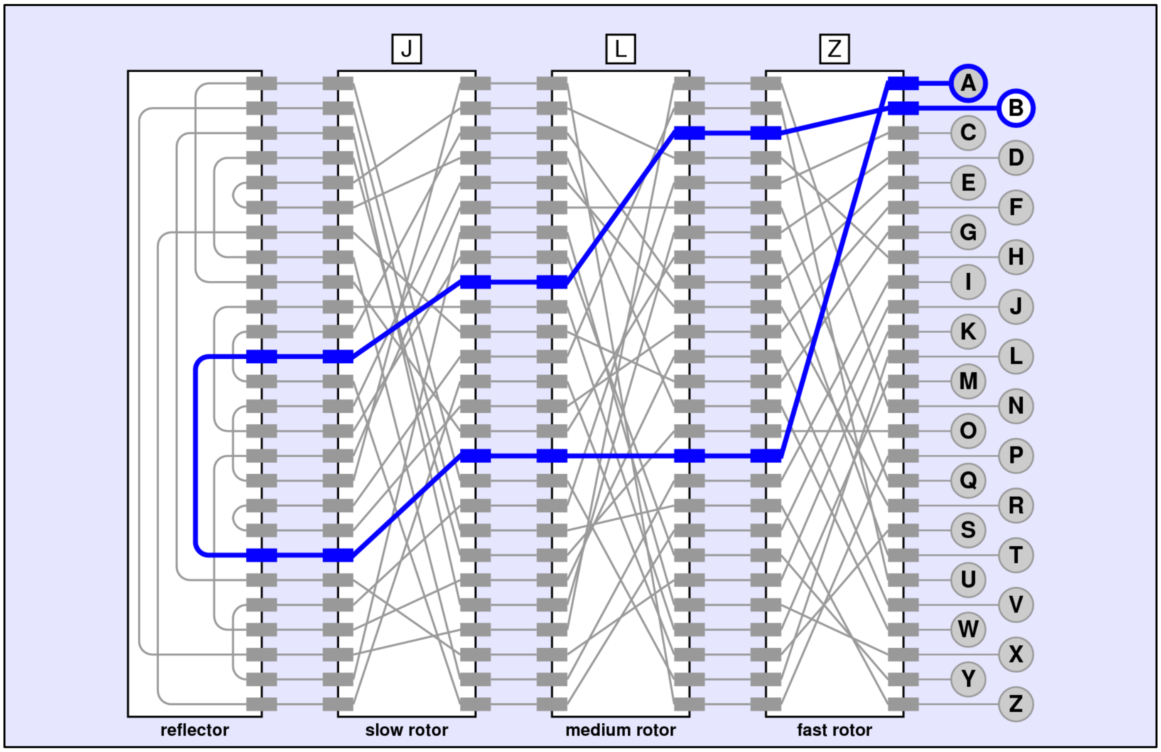
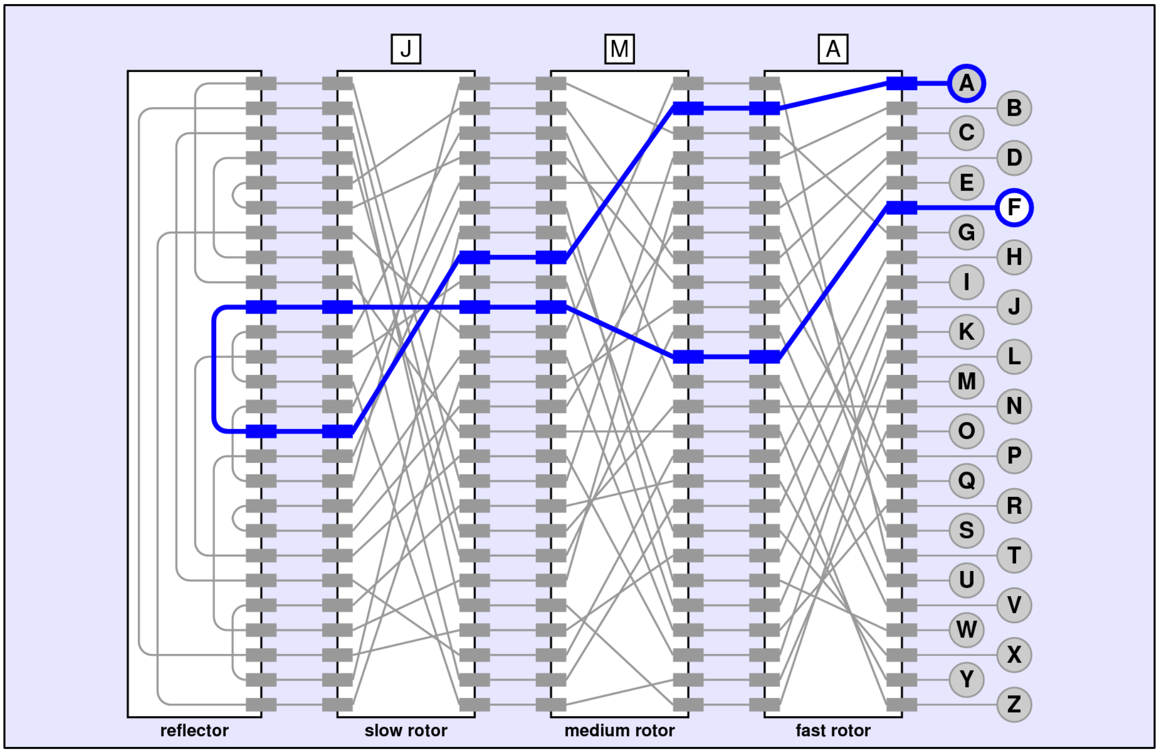


Figure 4. The Enigma machine after pressing the A key



alphabet and cycles back to **A**. Completing the cycle causes a "carry" to the medium rotor, which advances from **L** to **M**. Given the rotor setting **JMA**, the letter **A** is translated into the letter **F**, as shown in Figure 5.

Figure 5. The Enigma machine after pressing the A key a second time



At this point, it is useful to note a fundamental symmetry in the Enigma design. If **A** is transformed to **F** at some rotor setting, it must also be the case that **F** is transformed to **A**. The circuit is exactly the same; the only difference is that the current flows in the opposite direction. This symmetry is very useful for Enigma operators because it means that the sender and receiver don't need to have two different keys. The sender sets the rotors according to a codebook and types in the message. What comes out in the lights is the ciphertext, which is typically transmitted over a radio channel in Morse code. As long as the receiver uses the same codebook and sets up the machine in the same way, typing in the ciphertext restores the original message, because the encryption is reversible. As it happens, the fact that the encoding is reversible also makes it easier to break.

Learning more about breaking the Enigma code

Your goal in this assignment is to simulate the function of the Enigma machine, which was indeed one of the challenges that the codebreakers at Bletchley Park had to solve. If you're interested in how the Bletchley codebreakers managed to break Enigma, you can read the chapter on cryptography that appears in a book that Eric is writing about the great ideas in computing. That chapter is available on the CS 106J website.