Unit 177
Enigma

The *Enigma* is a cipher machine that was first invented for commercial use, but was used by Germany (and others) in World War II. No book on mechanical cryptography would be complete without a description of the machine and some of its variations, but for the history around the Enigma, we refer you to Kahn's books cited in the references.

The significant innovation in the Enigma is the use of *rotors* (also called *wheels*) to generate permutations of the alphabet in a very-long-period polyalphabetic substitution. This innovation spread beyond Germany and was incorporated into cipher machines in America, Russia, and elsewhere; in Units 179 and 180 we will look at two such machines. A *rotor* is a wheel with a pin for each letter of the alphabet on one side. On the other side are the same number of connections. Inside, the rotor has hidden wiring that connects each pin on one side to one connector on the other. The result is a permutation of the alphabet, whose letters are sent through the rotor with an electric current. When a rotor is rotated to a new position, the permutation changes. By putting several rotors in sequence, and by rotating them separately, the alphabetic permutation can be different for every character in the plaintext.

Figure 177.1: An Enigma with four rotors. Photo by Greg Goebel

The Enigma was originally configured to use three removable and replaceable rotors, and later the German navy added a fourth. There also was a removable and replaceable *reflector*, so that the signal for a letter of the plaintext left the keyboard, passed through the three rotors, the reflector, and the inverse of the three rotors, to emerge on a wire that lit an indicator representing the ciphertext letter (see Figure 177.2). The machine is laid out such that the signal enters the rightmost rotor first, which happens to be the one that we list last in the key. The rotor listed first is leftmost and closest to the reflector. The reflector by its very nature must have a self-reciprocal (involutory) (degree-2) permutation. The overall permutation of the machine is therefore also self-reciprocal. In the following equation in operator notation, we use U for the reflector ("Umkehrwalze" in German) and W for the rotors ("Walzen" in German), to distinguish them both from the symbol R that we use for the Caesar rotation. The current positions of the rotors are denoted with r. From the equation, we can see that the overall permutation is a conjugation of the reflector's permutation; therefore the overall permutation is also self-reciprocal and has degree 2.

$$c = E\,p = W_3(r_3)^{-1}\,W_2(r_2)^{-1}\,W_1(r_1)^{-1}\,U\,W_1(r_1)\,W_2(r_2)\,W_3(r_3)\,p = X^{-1}\,U\,X\,p \qquad (177.1)$$

Because of this property, a letter is never enciphered to itself; this weakness makes it easier to place cribs and helped cryptanalysts break the Enigma during the war. See Tables 177.1 and 177.2 for the permutations of the reflectors and rotors that are relevant to Germany and its military. For those models using four rotors, the reflector must be one of the thin ones, and the first rotor must be β (beta) or γ (gamma). In such machines, the first rotor is placed in a position specified by the key and does not rotate. Reflectors are always placed in the same position.

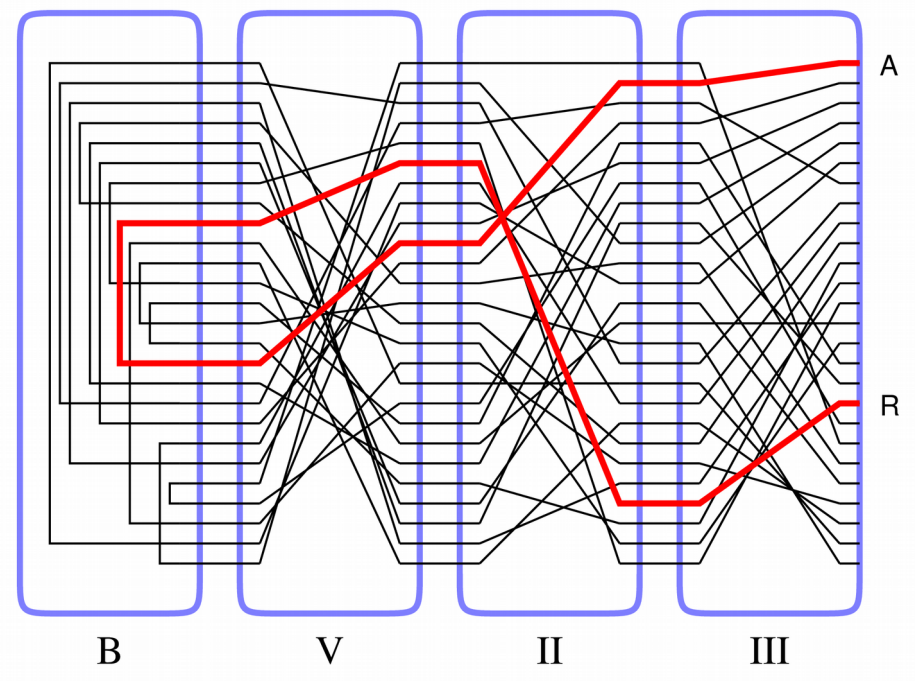

Figure 177.2: Diagram illustrating how the signal passes through the rotors and reflector of a three-rotor Enigma machine. The three rotors are all in position 0*. The path changes when one or more rotors advance.*

The β and γ rotors are thinner than the others, so that one of them with a thin reflector occupied the same width as one of the normal-sized reflectors. Furthermore, there are configurations of thin reflector with thin rotor that mimic the thick reflectors so that the four-rotor machine is backward-compatible with the three-rotor machine. In terms of alphabetic permutations, for this to occur, we need the thick reflector to be the conjugate of a thin reflector:

$$W_{\text{thin}}(0)^{-1}\, U_{\text{thin}}\, W_{\text{thin}}(0) \;=\; U_{\text{thick}} \tag{177.2}$$

The choices and positions of the thin components that satisfy Equation 177.2 are B thin with β in position 0 and C thin with γ in position 0, where by "position 0" we mean the position in which their effective alphabetic permutations are those that appear in Table 177.2.

We would like to point out that the rotation of a rotor is equivalent to sandwiching its operator between a Caesar rotation R of the alphabet and its inverse (look back at Unit 20):

$$W(r) \;=\; R(r)^{-1}\, W(0)\, R(r) \;=\; R(-r)\, W(0)\, R(r)$$

Then we can rewrite the encryption operator in Equation 177.1 as

$$\begin{aligned} E \;&=\; W_3(r_3)^{-1}\, W_2(r_2)^{-1}\, W_1(r_1)^{-1}\, U\, W_1(r_1)\, W_2(r_2)\, W_3(r_3) \\ &=\; R(-r_3)\, W_3(0)^{-1}\, R(r_3)\, R(-r_2)\, W_2(0)^{-1}\, R(r_2)\, R(-r_1)\, W_1(0)^{-1}\, R(r_1) \\ &\quad\; U\, R(-r_1)\, W_1(0)\, R(r_1)\, R(-r_2)\, W_2(0)\, R(r_2)\, R(-r_3)\, W_3(0)\, R(r_3) \\ &=\; R(-r_3)\, W_3(0)^{-1}\, R(r_3-r_2)\, W_2(0)^{-1}\, R(r_2-r_1)\, W_1(0)^{-1}\, R(r_1) \\ &\quad\; U\, R(-r_1)\, W_1(0)\, R(r_1-r_2)\, W_2(0)\, R(r_2-r_3)\, W_3(0)\, R(r_3) \end{aligned}$$

In other words, we can think of the rotors in the Enigma as remaining stationary, with changing Caesar shifts inserted between and aside them. Including the ring settings would have the same effect as changing the rotor positions in the above equation.

There is a further complication regarding the rotors. At first, the letter labels on their edges were printed directly onto them, but later they were printed on rings that could be fixed onto the rotors in different positions. This does not affect the way the alphabetic permutations are applied, but it does introduce offsets into the key (see below for how the key is specified) and does affect how the rotors advance between the encipherments of the plaintext letters (also see below regarding rotor advancement).

We must now discuss the rotation of the rotors in the Enigma machine. When the operator presses a key on the keyboard, the advancement of the rotors occurs before the plaintext letter is enciphered. The rightmost rotor (which is listed last in the key) advances one step every time a key is pressed. There are one or two notches on the rings for each rotor (except β and γ) that control the advancement of the rotor to its left. See Table 177.3 for the locations of the notches. Since beta and gamma can only be used as the rotor next to the reflector, they do not have these notches. If a rotor is in a notched position, then when it advances it causes the rotor to its left also to advance. The Enigma machine has a bug (which programmers now call a "feature") known as *double-stepping*: When the middle rotor reaches its notched position, then on the next key-press, it advances again along with the rotor to its left. For example, suppose that the rotors in use are I, II, and III. Rotor III is notched at position V, and rotor II at position E. So the middle rotor advances after the rightmost rotor reaches V,

as in ..., AAU, AAV, ABW, ABX, ... When rotor II reaches E, the double-stepping occurs, as in ..., ADU, ADV, AEW, BFX, BFY, ...

Later models had a *plugboard* ("Steckerbrett") that allowed the transposition of up to ten pairs of letters before they entered the rotors. After leaving the rotors, the plugboard applied the same transpositions again. This had the effect of adding another alphabetic permutation (*S*) to Equation 177.1:

$$c = S\, W_3(r_3)^{-1}\, W_2(r_2)^{-1}\, W_1(r_1)^{-1}\, U\, W_1(r_1)\, W_2(r_2)\, W_3(r_3)\, S\, p$$

We did not write "S^{-1}" on the left because *S* is its own inverse.

The encryption key of the Enigma consists of these things:

- the choice of reflector
- the choice of the three or four rotors and the order in which they are placed
- the ring setting for each rotor (one number [1-26] for each)
- the plugboard connections (a set of up to ten pairs of letters, with no repetition)
- the starting positions of the rotors (a sequence of three or four letters)

Typically, all but the last of these were configured each morning as the internal daily settings. The machine would be locked and only the starting positions of the rotors could be changed during the day. They served as the message key and were, ideally, different for each message during the course of any given day.

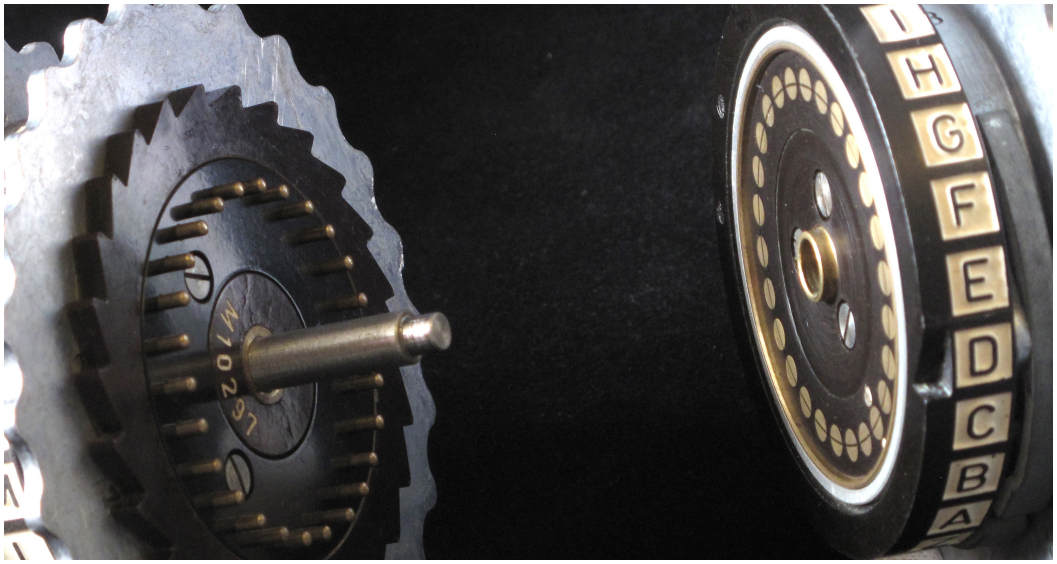

Figure 177.3: The two sides of rotors used in the Enigma. One side has pins, the other pads. The advancement notch is visible in the ring on the rotor to the right. Photo by Ted Coles.

Let’s try an example of encryption with the Enigma machine. Take this plaintext:

THISXMESSAGEXISXENCRYPTEDXWITHXTHEXENIGMA

and use the key B, II, I, VI, 5, 7, 9, GELATINOUS, GOO. On the first press of a key, the rightmost rotor (VI) advances to P and the keyboard emits a signal on the line representing T. The signal passes through the plugboard to emerge on the line for I, since (I T) is one of the transpositions specified in the key. Next, the signal enters rotor VI, but since the ring setting is 9 and the rotor is in position P, it enters the P pin (8−8+15 = 15 modulo 26, and we must take 1 less than the ring setting because we consider A to be zero). Rotor VI then emits its signal on the pad for R (see Table 177.2), which becomes K after we add the 8 and subtract the 15. The middle rotor (I) has its ring at 7 and is in position O, so we subtract 6 and add 14 to K to find that the signal enters on the S pin. The signal leaves rotor I on the S pad, which becomes K after we add the 6 and subtract the 14. The leftmost rotor (II) has ring setting 5 and is at position G, so we subtract 4 and add 6 to see that the signal enters on the M pin and leaves on the W pad. Adding the 4 and subtracting the 6 gives a signal entering reflector B on the U pin. The signal leaves the reflector on its C pin. Subtract 4 and add 6 to see that it enters the E pad of rotor II, so it leaves via the Z pin. Add back the 4 and subtract the 6, then subtract 6 and add 14, to find that the signal enters rotor I on the F pad and leaves on the D pin. Add back the 6 and subtract the 14, and subtract 8 and add 15, to find that it enters rotor VI on the C pad and leaves on the X pin. Add back the 8 and subtract 15 back into it to get a signal on the Q wire. The plugboard does not affect Q, so theis is the ciphertext letter. This painful process continues until the entire text is enciphered. The complete ciphertext is

QXRYIASMEJFZDGZMHYNBBRLFNRDEQDVPNMHAEJAYH

If you work through the details, you will notice that a double-stepping occurs when the D of ENCRYPTED and the following X are enciphered. The positions of the rotors go from GPM to GQN to HRO.

reflector	input ABCDEFGHIJKLMNOPQRSTUVWXYZ
A	EJMZALYXVBWFCRQUONTSPIKHGD
B	YRUHQSLDPXNGOKMIEBFZCWVJAT
C	FVPJIAOYEDRZXWGCTKUQSBNMHL
B thin	ENKQAUYWJICOPBLMDXZVFTHRGS
C thin	RDOBJNTKVEHMLFCWZAXGYIPSUQ

Table 177.1: Alphabetic permutations of the Enigma's reflectors. Later versions of the machine have a D *rotor whose wiring is changed as part of the key.*

rotor	input ABCDEFGHIJKLMNOPQRSTUVWXYZ
I	EKMFLGDQVZNTOWYHXUSPAIBRCJ
II	AJDKSIRUXBLHWTMCQGZNPYFVOE
III	BDFHJLCPRTXVZNYEIWGAKMUSQO
IV	ESOVPZJAYQUIRHXLNFTGKDCMWB
V	VZBRGITYUPSDNHLXAWMJQOFECK
VI	JPGVOUMFYQBENHZRDKASXLICTW
VII	NZJHGRCXMYSWBOUFAIVLPEKQDT
VIII	FKQHTLXOCBJSPDZRAMEWNIUYGV
β	LEYJVCNIXWPBQMDRTAKZGFUHOS
γ	FSOKANUERHMBTIYCWLQPZXVGJD

Table 177.2: Alphabetic permutations of the Enigma's rotors in position 0*. In the forward direction, input is on a pin and output on a pad.*

rotor	location of notch(es)
I	Q
II	E
III	V
IV	J
V	Z
VI	M, Z
VII	M, Z
VIII	M, Z

Table 177.3: Location of advancement notches on rotors in the Enigma.

Reading and references

Mark Stamp and Richard M. Low, *Applied Cryptanalysis: Breaking Ciphers in the Real World*, Hoboken: Wiley, 2007, section 2.2.

Wikipedia has many pages on the Enigma. Start with these:
https://en.wikipedia.org/wiki/Enigma_machine
https://en.wikipedia.org/wiki/Enigma_rotor_details

Philip Marks and Frode Weierud, "Recovering the Wiring of Enigma's *Umkehrwalze* A," *Cryptologia* 24:1 (2000) 55-66, https://doi.org/10.1080/0161-110091888781

David Kahn, *The Codebreakers: The Story of Secret Writing*, New York: Simon & Schuster, 1967, pages 420-423 and elsewhere, https://ia600606.us.archive.org/30/items/B-001-001-264/B-001-001-264.pdf, https://archive.org/details/B-001-001-264

David Kahn, *Seizing the Enigma: The Race to Break the German U-Boat Codes, 1939-1943*, New York: Houghton Mifflin, 1991.

Programming tasks

1. Simulate the Enigma in Python. Allow for the possibilities that either three or four rotors are used. Implement all reflectors and rotors that are presented in this unit.

Exercises

1. Decipher this ciphertext. The key is B, I, V, III, 5, 9, 15, PS, AY, IJ, ER, VN, MAX. An X has been placed between words in the plaintext, and XX between sentences.

```
LZJWKMOPGWGKESNUONOICEWIAULJIQTLRUZKAANKPWWGVQHRCWVZZERYGGZBBLCY
BSZWPLWGSVUWFRKGLHPRJDHJYOSTDPKRGAMJEZCNFMQGBAHYBALYMUJCPOOJGEDN
NKHBHMAFMUGLQDCYPESQZDIYOQWQSTZSUMDCMQSSXKHGYKMLTZKFDXYZCFXKWJZA
EPSVIZVUIQAVWGRJAW
```

2. Decipher this ciphertext. The key is C, II, IV, VI, 13, 25, 7, DECRYPTION, ABC. An X has been placed between words in the plaintext, and XX between sentences. This exercise will test your implementation of double-stepping.

```
TFELTJWHTSFJBHTRBBOWLHNRLMNDWHGZZIGNYHWKKWJQTNCKQQTNWNJRSWDJPGDM
ILQOIYPPYJUZFWCYZKPJZSWISAISUJECOQAHCFVUDJTQQRYEHVUGEIYHRMDBXNNB
IFOZDIARLAOXTFYMIWAPRACSFXZDXADRKJNJUVVVNZMLYZZOYAUCTMHIVVPYCXVI
DTQDEZGVEGMMTCXZUIGRUCRCDWDXEYHMSVVVKKLJWJWAWYONPYBUKWKBIESHKYYF
RGQAMDIXEBXWQSXLPG
```

3. Verify Equation 177.2 for U_{thick} = B, U_{thin} = B thin, W_{thin} = β in position 0 and for U_{thick} = C, U_{thin} = C thin, W_{thin} = γ in position 0.