Unit 184
Purple

The *Purple* machine was a cipher machine used by the Japanese during World War II. It gets its name from the purple binder in which American cryptanalysts kept their notes; its Japanese name was Kyunana-shiki obun injiki (九七式欧文印字機), which means "'97 European-character machine" ('97 denoted the year 2597 in the Japanese calendar). It was also called *Type B Cipher Machine*, as it was the successor to the Red (Type A) machine. The machine is different from the rotor and teleprinter machines: it uses switches to choose permutations, and therefore when a switch steps the new permutation is unrelated to the previous one.

The Japanese language is based on a syllabary, where every syllable ends in a vowel or N. To preserve this structure and so that ciphertexts can be pronounceable by cipher clerks, vowels and consonants are encrypted separately. Japanese uses two copies of the syllabary and thousands of Chinese characters; this makes the decision to use Latin letters seem sensible, and Red and Purple both encrypt messages transcribed into the twenty-six European letters. The vowels, `AEIOUY`, called "sixes" because there are six of them, are passed through one switch (the "sixes switch") that permutes them. The consonants (the "twenties") pass through three switches that permute them. See the tables at the end of this unit for the permutations of each switch, and Figure 184.2 for a diagram of the machine.

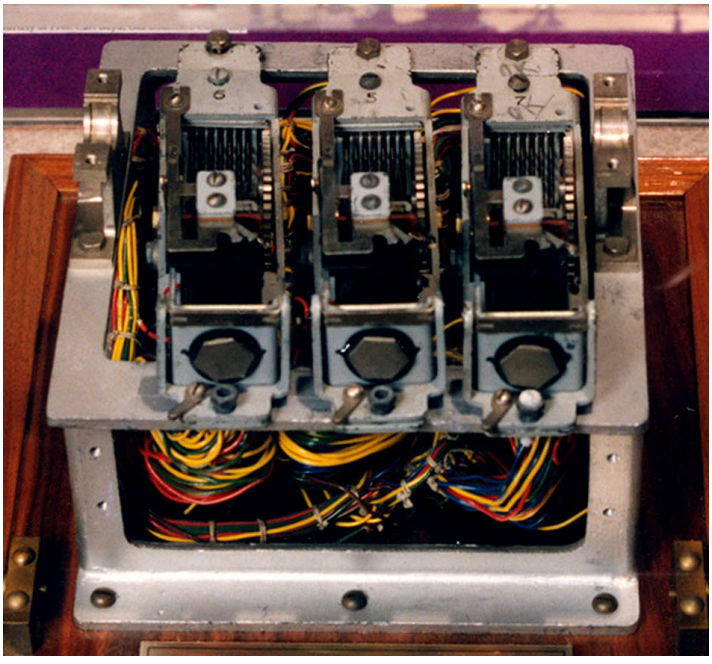

Figure 184.1: Largest surviving piece of a Purple machine. Photo from United States Air Force.

The way the machine works is as follows. The operator presses a button on the keyboard for the plaintext letter. This sends a signal on the wire for that letter. If it is one of the sixes, then it enters the sixes switch. Based on the position of that switch, the signal leaves the sixes switch on another line. The permutations for each of the twenty-five positions of the switch are in Table 184.1. If the plaintext letter is one of the twenties, then the signal is permuted by three switches. First is the “left” switch, then the “middle” switch, and finally the “right” switch. The output of the right switch leaves the machine. Each of the three twenties switches has twenty-five positions, and each position gives a different permutation of the twenty letters; see Tables 184.2, 184.3, and 184.4 for the permutations. After each letter is enciphered, the sixes switch advances to the next position. Before operation, the three twenties switches are assigned to the rôles of “fast” switch, “medium” switch, and “slow” switch. Whichever is the fast switch advances by one after each letter is enciphered. When the sixes switch advances from 24 to 25, the medium twenties switch advances by one. When the sixes switch advances from 23 to 24 and the medium switch advances from 24 to 25, the slow switch advances by one. Any switch that advances from position 25 comes around back to position 1.

Purple inherited its split of the alphabet into sixes and twenties from its predecessor, Red. However, the feature becomes moot with the introduction of a plugboard that permutes all twenty-six letters on the way into the machine and inversely on the way out. The full machine (P) is a conjugation of the bare unplugged machine (U) is between the monoalphabetic substitution (S) and its inverse:

$$c = P\,p = S^{-1}\,U\,S\,p$$

If it is not obvious, we tell you that the substitution shuffles which letters are the sixes and which are the twenties.

The key for Purple consists of these things:

- the initial position of the sixes switch (one number)
- the initial positions of the twenties switches (three numbers)
- the choices of which of the twenties switches are slow, medium, fast
- permutation on the plugboard (simetimes split into sixes and twenties)

For example, our key might be

sixes:	21				
left:	4	middle:	18	right:	9
fast:	middle	medium:	right	slow:	left
plugboard:	TQCLNR PSBYGJZMFOWUDKVHAEXI				

If we split the plugboard into sixes and twenties this way, then what we mean is the inverse permutation, so that TQCLNR → AEIOUY and PSBYGJZMFOWUDKVHAEXI → BCDFGHJKLMNPQRSTVWXZ. We should always try to be clear on exactly what we mean when we give a plugboard permutation for Purple. With this key, let us encipher the text

THIS MESSAGE ENCRYPTED WITH PURPLE

The first letter, `T`, is translated to `A` by the plugboard. This is one of the sixes, and from Table 184.1, we see that a signal on line 1 emerges from the sixes switch on line 3, so this letter is enciphered to `I`. The plugboard translates it to `C`. After the first letter is enciphered, the sixes switch advances to 22 and the fast twenties switch (middle) advances to 19. The second plaintext letter, `H`, is mapped to `T` by the plugboard, which is on line 16 entering the left twenties switch. From Table 184.2 we see that it emerges on line 6. The signal enters the middle switch and emerges on line 16. This enters the right switch and emerges on line 19. The plugboard translates this to `X`. The full ciphertext is

```
CXEEEKVXMSXBNNRDEQEZEHLAAUCOTE
```

Without the plugboard, we would get

```
CBURDAWMOCAODJHURHEVBODBLEHFXE
```

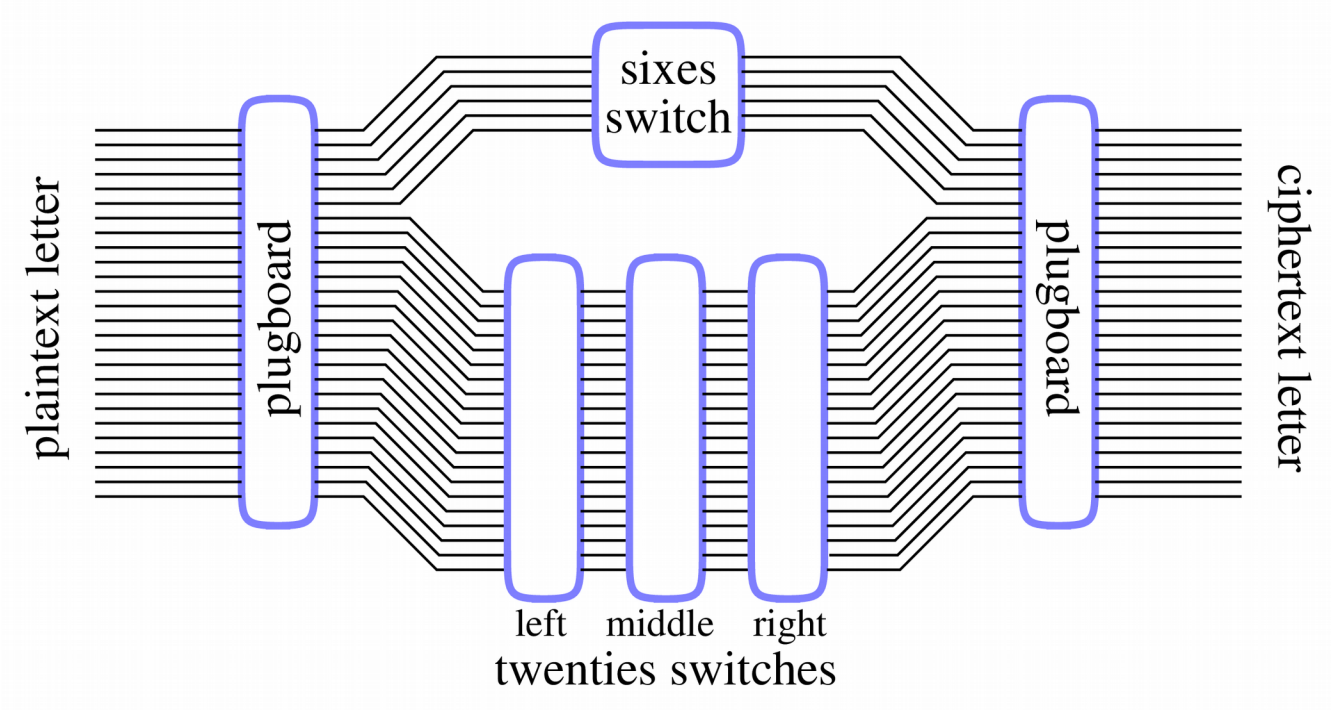

Figure 184.2: Diagram of the Purple machine.

switch position	**input** 1 2 3 4 5 6
1	2 1 3 5 4 6
2	5 4 2 6 3 1
3	1 5 6 3 2 4
4	4 3 2 1 6 5
5	3 6 1 4 5 2
6	2 1 5 6 4 3
7	5 4 6 3 2 1
8	3 6 1 4 5 2
9	6 3 5 2 1 4
10	5 4 3 1 2 6
11	2 1 6 3 4 5
12	6 5 4 2 1 3
13	2 3 1 5 6 4
14	4 2 5 1 3 6
15	1 3 4 6 5 2
16	5 6 3 2 1 4
17	6 2 4 5 3 1
18	4 1 2 3 5 6
19	1 2 3 6 4 5
20	2 5 1 4 6 3
21	3 4 6 5 2 1
22	1 5 2 4 6 3
23	4 6 5 2 3 1
24	3 4 6 1 5 2
25	6 2 4 3 1 5

Table 184.1: Permutations of the sixes switch of the Purple machine.

switch position	**input**																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	4	7	13	6	17	1	8	11	10	5	16	18	9	3	15	12	20	14	2	19
2	6	17	9	1	2	18	20	10	19	15	12	13	14	5	8	3	4	11	16	7
3	2	19	12	17	20	4	13	15	18	11	6	8	3	14	5	9	1	10	7	16
4	14	9	1	4	13	5	17	7	12	16	15	10	18	2	19	6	11	20	8	3
5	19	16	10	8	6	2	15	3	20	9	18	14	5	13	12	11	17	7	1	4
6	20	1	8	18	19	7	5	12	3	13	2	11	10	4	14	15	16	9	6	17
7	8	10	19	12	11	3	2	17	5	6	13	20	7	16	18	1	9	4	14	15
8	1	20	14	15	7	12	3	13	16	10	17	5	11	6	9	4	18	8	19	2
9	9	14	20	17	12	15	7	4	2	18	3	16	19	8	11	10	1	6	13	5
10	17	13	5	7	10	16	11	2	4	8	20	1	15	9	19	14	3	12	18	6
11	2	5	13	8	16	17	18	9	7	11	4	19	12	15	10	3	6	14	20	1
12	18	4	16	2	1	7	12	11	17	14	19	9	5	10	3	8	13	15	6	20
13	16	6	11	20	17	19	10	8	9	3	7	15	14	12	1	5	2	13	4	18
14	13	11	4	9	12	8	3	5	14	17	1	2	20	18	6	7	19	16	15	10
15	10	3	18	5	9	15	4	6	12	20	11	1	17	16	7	2	14	19	8	13
16	4	17	15	16	18	20	14	1	13	19	6	5	11	8	2	10	7	3	12	9
17	15	13	2	19	3	14	1	20	11	12	10	17	6	9	16	18	5	4	7	8
18	12	7	6	3	19	13	16	18	15	1	9	14	2	4	17	20	8	5	10	11
19	11	12	16	14	15	10	2	19	3	8	13	4	1	7	20	6	18	17	9	5
20	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
21	7	18	12	11	4	20	9	14	1	5	16	3	8	19	10	13	6	15	17	2
22	5	3	17	18	8	11	6	16	13	7	14	15	4	20	2	19	10	1	9	12
23	9	16	19	10	7	14	13	20	8	4	5	11	12	17	18	1	15	2	3	6
24	3	8	10	13	1	9	19	2	6	18	20	7	16	11	4	15	12	17	5	14
25	19	15	7	3	14	12	18	4	5	2	8	6	20	1	13	17	9	16	11	10

Table 184.2: Permutations of the left twenties switch of the Purple machine.

switch position	input																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	3	8	7	18	4	15	20	10	2	9	11	13	16	19	1	14	5	12	6	17
2	17	4	20	5	11	2	14	7	6	15	12	1	19	18	3	8	10	16	9	13
3	6	14	18	1	3	17	15	4	16	19	13	7	11	10	8	5	12	2	20	9
4	14	3	10	19	12	1	6	11	17	13	2	8	20	5	9	18	15	7	16	4
5	9	2	4	6	17	13	1	18	5	20	14	10	3	8	16	15	7	11	19	12
6	11	12	14	15	1	19	4	9	6	5	17	16	10	3	20	13	2	18	7	8
7	18	7	3	2	20	16	19	1	8	11	4	9	6	13	14	10	12	17	5	15
8	2	17	11	16	10	20	12	6	18	4	8	19	13	7	5	3	14	9	15	1
9	10	6	17	7	5	12	3	2	1	16	11	20	8	15	4	19	9	14	13	18
10	17	20	12	13	9	10	16	5	11	1	3	2	15	18	19	6	8	4	14	7
11	8	16	20	4	13	7	2	19	14	18	1	11	9	3	12	15	17	5	10	6
12	15	1	2	20	16	14	9	17	3	4	10	12	5	6	7	8	18	13	19	11
13	4	13	6	9	15	11	10	12	8	2	16	17	7	14	3	1	5	19	18	20
14	19	10	5	14	18	9	15	20	7	8	13	4	6	12	17	2	11	3	1	16
15	5	19	17	16	11	8	6	13	12	7	9	3	18	2	10	20	15	1	4	14
16	20	4	2	5	6	18	16	15	9	10	7	14	17	8	13	12	19	11	3	1
17	13	5	1	3	8	2	11	16	15	17	18	6	19	4	14	7	20	9	12	10
18	7	12	19	11	1	14	13	18	4	5	15	10	9	16	2	17	6	20	8	3
19	12	9	15	8	5	16	17	7	13	18	20	19	3	1	10	11	4	6	14	2
20	3	18	10	17	7	4	19	1	20	11	2	13	12	6	15	16	9	8	5	14
21	4	15	11	18	19	3	8	17	10	14	12	5	13	20	6	9	1	16	2	7
22	1	20	13	12	2	5	10	8	9	15	6	3	14	7	19	18	16	17	11	4
23	16	14	9	10	8	6	18	2	19	3	5	20	4	17	11	1	13	15	7	12
24	8	9	16	20	14	12	7	3	13	6	19	15	2	11	18	4	17	10	1	5
25	2	11	8	6	10	20	5	14	16	12	15	18	1	9	4	7	3	13	17	19

Table 184.3: Permutations of the middle twenties switch of the Purple machine.

switch position	**input**																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	6	20	4	15	17	8	1	13	14	7	3	10	12	18	19	9	11	16	2	5
2	9	4	8	12	20	18	14	7	11	13	15	5	6	3	1	17	2	19	10	16
3	5	1	14	7	19	11	15	18	9	8	2	4	13	10	12	16	20	17	6	3
4	16	10	2	5	11	7	20	12	4	15	14	3	19	13	17	1	18	9	8	6
5	18	12	6	4	15	9	13	11	5	14	20	1	8	17	7	3	19	2	16	10
6	19	13	18	17	3	4	6	5	2	12	15	7	1	9	16	20	8	10	14	11
7	11	3	13	1	8	15	2	9	18	6	19	12	14	16	4	10	5	20	7	17
8	12	17	20	3	9	2	19	7	1	4	18	10	15	8	14	6	11	5	16	13
9	13	14	11	16	1	12	9	10	17	18	7	8	5	2	6	19	4	3	20	15
10	10	13	5	14	7	16	18	17	3	9	1	6	19	11	8	2	12	4	15	20
11	7	9	3	18	6	20	16	2	19	10	8	11	17	5	4	12	15	13	1	14
12	1	8	15	10	11	13	6	16	5	20	12	2	4	7	9	14	3	17	18	19
13	5	7	1	2	19	14	12	8	16	3	20	4	10	9	15	13	17	6	11	18
14	17	12	20	6	4	3	11	19	1	5	2	13	9	15	10	18	7	14	8	16
15	15	18	10	13	17	19	8	1	12	9	16	6	2	3	11	4	14	20	5	7
16	16	5	19	4	14	9	18	17	15	20	10	8	7	13	3	2	6	1	12	11
17	2	15	16	11	13	5	3	20	10	17	14	9	6	1	18	7	12	8	19	4
18	3	6	9	8	12	17	5	10	16	11	4	14	18	20	13	15	1	7	2	19
19	8	3	12	20	18	6	7	14	13	1	5	19	11	4	2	9	16	15	17	10
20	20	7	14	9	8	4	10	3	2	16	6	5	17	12	15	11	13	19	18	1
21	13	19	17	12	16	10	15	4	18	6	1	20	3	8	11	5	14	7	9	2
22	9	11	10	5	2	14	17	15	20	3	13	18	16	19	7	1	8	6	4	12
23	7	16	19	10	5	1	13	18	6	2	11	17	15	14	20	4	9	12	3	8
24	4	18	15	17	3	12	2	1	7	19	9	16	20	6	5	8	10	11	13	14
25	14	2	7	19	10	13	4	6	8	12	17	15	1	5	16	11	3	18	20	9

Table 184.4: Permutations of the right twenties switch of the Purple machine.

Reading and References

Mark Stamp and Richard M. Low, *Applied Cryptanalysis: Breaking Ciphers in the Real World*, Hoboken: Wiley, 2007, section 2.3.

William F. Friedman, Preliminary Historical Report on the Solution of the "B" Machine, https://cryptocellar.org/files/purple-history.pdf

Barjol Lami, Gledis Kallco, Nicholas Guo, and Sean Shi; "Cryptanalysis of Purple, Japanese WWII Cipher Machine," 2019, https://courses.csail.mit.edu/6.857/2019/project/24-Lami-Kallco-Guo-Shi.pdf

Wes Freeman, Geoff Sullivan, and Frode Weierud, "Purple Revealed: Simulation and Computer-Aided Cryptanalysis of Angooki Taipu B," *Cryptologia* 27:1 (2003) 1-43, DOI: 10.1080/0161-110391891739

Kenneth J. Bures, "Cracking PURPLE: cryptanalysis of the Angooki Taipu B switch tables," *Cryptologia* 45:1 (2021) 1-43, DOI: 10.1080/01611194.2019.1706064

Kenneth J. Bures, "Cracking PURPLE: the identification of homologs in the cryptanalysis of the Angooki Taipu B cipher machine," *Cryptologia* 47:5 (2023) 436-448, DOI: 10.1080/01611194.2022.2064200

Wikipedia, "Type B Cipher Machine," https://en.wikipedia.org/wiki/Type_B_Cipher_Machine

David Kahn, *The Codebreakers: The Story of Secret Writing*, New York: Simon & Schuster, 1967, pages 18-24 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

Programming tasks

1. Simulate the Purple machine cipher. Check that it can reproduce the examples in this unit.

Exercises

1. Encipher this text from with the example key given in this unit (with the plugboard).

   > The flowers were white, with streaks of golden orange upon the petals; the heavy labellum was coiled into an intricate projection, and a wonderful bluish purple mingled there with the gold. He could see at once that the genus was altogether a new one. And the insufferable scent! How hot the place was! The blossoms swam before his eyes.
   >
   > (from “The Strange Orchid” by H. G. Wells)

2. Decipher this ciphertext with the example key given in this unit (with the plugboard).

   ```
   DBVCUQNJMCHFYRNSOLJFPTLIRTUIAHWXTNPVIVFMSVSCESFRBSHVCCGHNWSQEPYL
   ORQUSFUFSXLPPTZMRFYRVQEALHZTJNMGIKLDWUHZPJHQECYCLFFLTDTITRGBTACC
   ANWKGLODVLSVPCXFPTLIKWTGYQELUTSDKZMQZGARYDCSPJYFTOSIYTKAVLRWKXZP
   SJDENHMFBDHZRUCUDSRUGLWJCYUOWRSTCPVJJTZZOYACBYTGDTABLQPNPUQKLSBQ
   KMTJYCJVONEJEDXXNKAJTEZPQARNSQRMXSITWLWQNJBCALDCJEXTTPEIXZVBTXLE
   YARMGXJVCYOXLVPQ
   ```