Unit 184
Siemens and Halske T52

The Siemens and Halske model T52 (code-named “Sturgeon” by British analysts) was an encryption machine that acted on the output (for encryption) or input (decryption) to a teleprinter. A teleprinter used five data lines and encoded/decoded its messages in Baudot (see Unit 183). The T52 performed two sorts of operations on the data in those five lines: it could flip a bit (change it from 0 to 1 or from 1 to 0), or it could swap two bits. Which bits were flipped and which were swapped was determined by ten wheels and some circuitry. Unlike the wheels in machines like the Enigma, the wheels of the T52 did not act on letters directly; rather, they provided control signals to the circuitry that performed operations on the five bits of the Baudot-encoded characters. The output of each wheel is mapped to the control of one bit operation by something like a plugboard and optionally some additional circuitry. There were five versions of the machine, which we will examine below; they differ in how the wheels rotate and in what additional circuitry they have.

The ten wheel are designated A, B, C, D, E, F, G, H, J, and K (“I” was skipped, probably because it looks like a Roman numeral). Each has its own number of positions: 73, 71, 69, 67, 65, 64, 61, 59, 53, and 47, respectively. These numbers are all coprime, so that if the wheels advance regularly (one step each after encrypting each character, as in some versions of the machine), then they will not return to their original configuration until 893,622,318,929,520,960 characters have been encrypted. At the time that the machine was in use, that was considered a big number. The wheels have pins that determine whether it emits a control signal that is active (“on” or “1”) or inactive (“off” or “0”) for each of its positions, which are numbered, starting from 1. The pin patterns of the ten wheels are given in Table 184.1.

A	·××·×××···×··××··×··××××··×××·×·×·×××··××··×××·××·····×××···××××·×·····×
B	·××××··××××××···×···×·×··××·×××××·····×××···××·×××·····××·×·×·×××·····×
C	·×××××·×·××··×·××····××·×····××××·×××·×××···×··×··×××····××····××···×
D	·××·×·×···×××·····××·×····×··×××··×××··×·×××···××··×··×·××××··×···×
E	·×···×···×·×××××××·×·××××××··×·×··××·×····×·×××××··×××·×·×·××···×
F	·×·×·×××××····×·××××··×·××·××××·××··×××····×····×××·××××××···×·×
G	·××××···××··××···×·×××××·×··×··×××·×·××·×·××·×····××·×··×·×××
H	·×··×××××···××××·×··××××···××·×···××·×·××···××××××··××·×·××
J	·×·××·××··××·×·××···×××···×××··×·×××·×····××××···×·××
K	·×····×××××···×··×·×××··×·×·×××··×××·××××···×××

Table 184.1: Pin patterns of the wheels of the T52. A cross indicates an active position (pin is present), and a dot indicates an inactive position (no pin). The first dot is at position 1.

Bit-flipping is done by five exclusive-or logic circuits. Exclusive OR (XOR) takes two input bits and outputs a 1 if and only if exactly one input is 1. Otherwise, the output is 0. See Table 184.2. The symbol for XOR is usually taken to be $\oplus$, since it has a close relationship with addition modulo 2 (see Unit 19) (actually, it *is* addition modulo 2). In the T52, the two inputs to an XOR circuit are a bit of the plaintext character and a control wire. Those control wires are labeled “I” for the circuit that acts on the first bit, “II” for the second, “III,” “IV,” and “V.” So the first bit is flipped if the control wire I is active, the second if II is active, etc.

inputs	output of OR	output of XOR
0 0	0	0
0 1	1	1
1 0	1	1
1 1	1	0

Table 184.2: The OR *and exclusive* OR *(*XOR*) operations, from Tables 181.3 and 181.4. The output of* OR *is on if either input is on. The output of* XOR *is on if and only if exactly one input is on.*

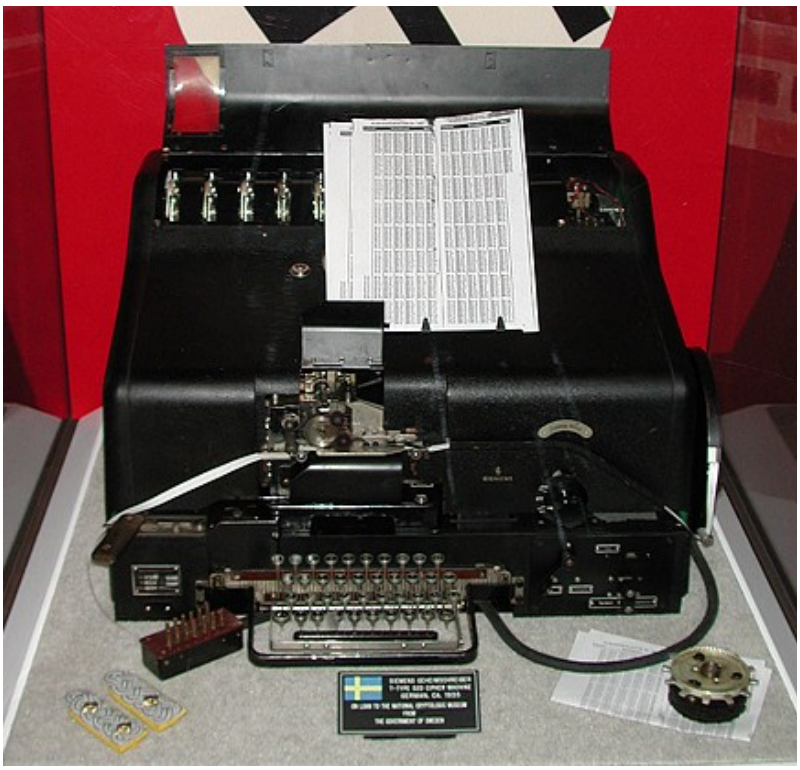

Figure 184.1: Siemens and Halske T52 version D on display at the U.S. National Cryptologic Museum. Photo credit: U.S. National Security Agency.

Bit-swapping is performed by relays that connect to the data lines and which are controlled by the control lines from the wheels in such a way that if the control line is active (1) then the bits are not swapped, but if the control line is inactive (0) then they are. There are five such relays, and each can be plugged into the data lines at two points. Therefore, we need ten points of access to the data; they are numbered and displayed schematically in Figure 184.2. A relay plugged into points 1 and 5, for example, can swap the bits on lines 1 and 4. This swapping comes *after* a swap that is wired to points 4 and 6, for example. Any possible wiring of the permutation circuit can be represented as five transpositions (swappings) in a definite order. For example, the fixed standard wiring of version C of the machine is 1-2, 3-4, 5-6, 7-8, 9-10, which corresponds to transpositions (1 5), (4 5), (3 4), (2 3), and (1 2), in that order.

There are 5! = 120 possible permutations of five bits. However, with five transpositions, there are only $2^5 = 32$ that can be implemented. There happen to be 120 ways to wire the swapping relays so that 32 permutations can be enacted, and there are 240 ways to wire them so that 30 permutations are possible. These 360 wirings were considered acceptable by the Germans, and we have listed them in Table 184.3. Any wiring not listed would result in fewer possible permutations or in loops in the data lines that disrupt the operation of the machine.

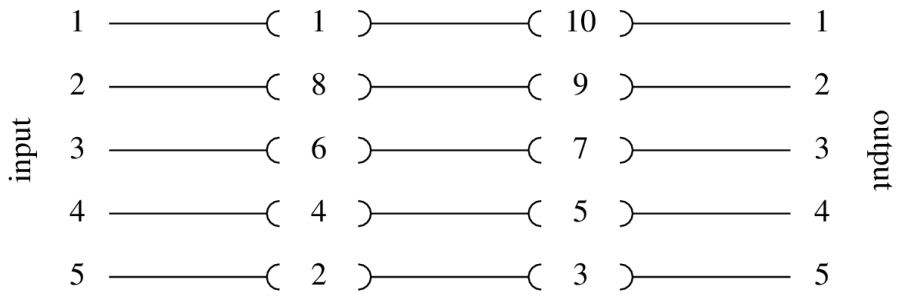

Figure 184.2: Schematic diagram of the access points and their labels for the swapping relays in the permutation circuitry. For example, a relay plugged into points 1 and 5 controls the swapping of bits 1 and 4.

The rest of this section is divided into subsections for each of the five versions of the T52. They all use the same wheels, the same XOR circuitry, and the same permutation circuitry. However, some fix the wiring of the swapping relays so that the permutation circuitry cannot be changed. Some versions introduce new features, such as additional logic circuitry between the wheels and the operations on the data bits, or irregular stepping of the wheels.

1-2 3-4 5-6 7-8 9-10	1-2 3-4 5-6 7-9 8-10	1-2 3-4 5-7 6-8 9-10	1-2 3-4 5-7 6-9 8-10	1-2 3-4 5-8 6-10 7-9
1-2 3-4 5-8 6-9 7-10	1-2 3-4 5-9 6-10 7-8	1-2 3-4 5-9 6-8 7-10	1-2 3-5 4-6 7-8 9-10	1-2 3-5 4-6 7-9 8-10
1-2 3-5 4-7 6-8 9-10	1-2 3-5 4-7 6-9 8-10	1-2 3-5 4-8 6-10 7-9	1-2 3-5 4-8 6-9 7-10	1-2 3-5 4-9 6-10 7-8
1-2 3-5 4-9 6-8 7-10	1-2 3-6 4-10 5-8 7-9	1-2 3-6 4-10 5-9 7-8	1-2 3-6 4-7 5-8 9-10	1-2 3-6 4-7 5-9 8-10
1-2 3-6 4-8 5-10 7-9	1-2 3-6 4-8 5-7 9-10	1-2 3-6 4-9 5-10 7-8	1-2 3-6 4-9 5-7 8-10	1-2 3-7 4-10 5-8 6-9
1-2 3-7 4-10 5-9 6-8	1-2 3-7 4-6 5-8 9-10	1-2 3-7 4-6 5-9 8-10	1-2 3-7 4-8 5-10 6-9	1-2 3-7 4-8 5-6 9-10
1-2 3-7 4-9 5-10 6-8	1-2 3-7 4-9 5-6 8-10	1-2 3-8 4-10 5-6 7-9	1-2 3-8 4-10 5-7 6-9	1-2 3-8 4-6 5-10 7-9
1-2 3-8 4-6 5-9 7-10	1-2 3-8 4-7 5-10 6-9	1-2 3-8 4-7 5-9 6-10	1-2 3-8 4-9 5-6 7-10	1-2 3-8 4-9 5-7 6-10
1-2 3-9 4-10 5-6 7-8	1-2 3-9 4-10 5-7 6-8	1-2 3-9 4-6 5-10 7-8	1-2 3-9 4-6 5-8 7-10	1-2 3-9 4-7 5-10 6-8
1-2 3-9 4-7 5-8 6-10	1-2 3-9 4-8 5-6 7-10	1-2 3-9 4-8 5-7 6-10	1-3 2-4 5-6 7-8 9-10	1-3 2-4 5-6 7-9 8-10
1-3 2-4 5-7 6-8 9-10	1-3 2-4 5-7 6-9 8-10	1-3 2-4 5-8 6-10 7-9	1-3 2-4 5-8 6-9 7-10	1-3 2-4 5-9 6-10 7-8
1-3 2-4 5-9 6-8 7-10	1-3 2-5 4-6 7-8 9-10	1-3 2-5 4-6 7-9 8-10	1-3 2-5 4-7 6-8 9-10	1-3 2-5 4-8 6-10 7-9
1-3 2-5 4-8 6-9 7-10	1-3 2-5 4-9 6-8 7-10	1-3 2-6 4-10 5-8 7-9	1-3 2-6 4-10 5-9 7-8	1-3 2-6 4-7 5-8 9-10
1-3 2-6 4-7 5-9 8-10	1-3 2-6 4-8 5-10 7-9	1-3 2-6 4-8 5-7 9-10	1-3 2-6 4-9 5-10 7-8	1-3 2-6 4-9 5-7 8-10
1-3 2-7 4-10 5-9 6-8	1-3 2-7 4-6 5-8 9-10	1-3 2-7 4-6 5-9 8-10	1-3 2-7 4-8 5-10 6-9	1-3 2-7 4-8 5-6 9-10
1-3 2-7 4-9 5-10 6-8	1-3 2-8 4-10 5-6 7-9	1-3 2-8 4-10 5-7 6-9	1-3 2-8 4-6 5-10 7-9	1-3 2-8 4-6 5-9 7-10
1-3 2-8 4-7 5-10 6-9	1-3 2-8 4-7 5-9 6-10	1-3 2-8 4-9 5-6 7-10	1-3 2-8 4-9 5-7 6-10	1-3 2-9 4-10 5-7 6-8
1-3 2-9 4-6 5-10 7-8	1-3 2-9 4-6 5-8 7-10	1-3 2-9 4-7 5-10 6-8	1-3 2-9 4-8 5-6 7-10	1-3 2-9 4-8 5-7 6-10
1-4 2-10 3-6 5-8 7-9	1-4 2-10 3-6 5-9 7-8	1-4 2-10 3-7 5-8 6-9	1-4 2-10 3-7 5-9 6-8	1-4 2-10 3-8 5-6 7-9
1-4 2-10 3-8 5-7 6-9	1-4 2-10 3-9 5-6 7-8	1-4 2-10 3-9 5-7 6-8	1-4 2-5 3-6 7-8 9-10	1-4 2-5 3-6 7-9 8-10
1-4 2-5 3-7 6-8 9-10	1-4 2-5 3-7 6-9 8-10	1-4 2-5 3-8 6-10 7-9	1-4 2-5 3-8 6-9 7-10	1-4 2-5 3-9 6-10 7-8
1-4 2-5 3-9 6-8 7-10	1-4 2-6 3-10 5-8 7-9	1-4 2-6 3-10 5-9 7-8	1-4 2-6 3-5 7-8 9-10	1-4 2-6 3-5 7-9 8-10
1-4 2-6 3-8 5-7 9-10	1-4 2-6 3-8 5-9 7-10	1-4 2-6 3-9 5-7 8-10	1-4 2-6 3-9 5-8 7-10	1-4 2-7 3-10 5-8 6-9
1-4 2-7 3-10 5-9 6-8	1-4 2-7 3-5 6-8 9-10	1-4 2-7 3-5 6-9 8-10	1-4 2-7 3-8 5-6 9-10	1-4 2-7 3-8 5-9 6-10
1-4 2-7 3-9 5-6 8-10	1-4 2-7 3-9 5-8 6-10	1-4 2-8 3-10 5-6 7-9	1-4 2-8 3-10 5-7 6-9	1-4 2-8 3-5 6-10 7-9
1-4 2-8 3-5 6-9 7-10	1-4 2-8 3-6 5-7 9-10	1-4 2-8 3-6 5-9 7-10	1-4 2-8 3-7 5-6 9-10	1-4 2-8 3-7 5-9 6-10
1-4 2-9 3-10 5-6 7-8	1-4 2-9 3-10 5-7 6-8	1-4 2-9 3-5 6-10 7-8	1-4 2-9 3-5 6-8 7-10	1-4 2-9 3-6 5-7 8-10
1-4 2-9 3-6 5-8 7-10	1-4 2-9 3-7 5-6 8-10	1-4 2-9 3-7 5-8 6-10	1-5 2-10 3-6 4-8 7-9	1-5 2-10 3-7 4-8 6-9
1-5 2-10 3-7 4-9 6-8	1-5 2-10 3-8 4-6 7-9	1-5 2-10 3-9 4-6 7-8	1-5 2-10 3-9 4-7 6-8	1-5 2-4 3-6 7-8 9-10
1-5 2-4 3-6 7-9 8-10	1-5 2-4 3-7 6-8 9-10	1-5 2-4 3-7 6-9 8-10	1-5 2-4 3-8 6-10 7-9	1-5 2-4 3-8 6-9 7-10
1-5 2-4 3-9 6-10 7-8	1-5 2-4 3-9 6-8 7-10	1-5 2-6 3-10 4-8 7-9	1-5 2-6 3-10 4-9 7-8	1-5 2-6 3-4 7-8 9-10
1-5 2-6 3-4 7-9 8-10	1-5 2-6 3-8 4-7 9-10	1-5 2-6 3-8 4-9 7-10	1-5 2-6 3-9 4-7 8-10	1-5 2-6 3-9 4-8 7-10
1-5 2-7 3-10 4-8 6-9	1-5 2-7 3-10 4-9 6-8	1-5 2-7 3-4 6-8 9-10	1-5 2-7 3-8 4-6 9-10	1-5 2-7 3-9 4-6 8-10
1-5 2-7 3-9 4-8 6-10	1-5 2-8 3-10 4-6 7-9	1-5 2-8 3-10 4-7 6-9	1-5 2-8 3-4 6-10 7-9	1-5 2-8 3-4 6-9 7-10
1-5 2-8 3-6 4-7 9-10	1-5 2-8 3-6 4-9 7-10	1-5 2-8 3-7 4-6 9-10	1-5 2-8 3-7 4-9 6-10	1-5 2-9 3-10 4-6 7-8
1-5 2-9 3-10 4-7 6-8	1-5 2-9 3-4 6-8 7-10	1-5 2-9 3-6 4-8 7-10	1-5 2-9 3-7 4-6 8-10	1-5 2-9 3-7 4-8 6-10
1-6 2-10 3-4 5-8 7-9	1-6 2-10 3-4 5-9 7-8	1-6 2-10 3-5 4-8 7-9	1-6 2-10 3-5 4-9 7-8	1-6 2-10 3-8 4-7 5-9
1-6 2-10 3-8 4-9 5-7	1-6 2-10 3-9 4-7 5-8	1-6 2-10 3-9 4-8 5-7	1-6 2-4 3-10 5-8 7-9	1-6 2-4 3-10 5-9 7-8
1-6 2-4 3-7 5-8 9-10	1-6 2-4 3-7 5-9 8-10	1-6 2-4 3-8 5-10 7-9	1-6 2-4 3-8 5-7 9-10	1-6 2-4 3-9 5-10 7-8
1-6 2-4 3-9 5-7 8-10	1-6 2-5 3-10 4-8 7-9	1-6 2-5 3-10 4-9 7-8	1-6 2-5 3-7 4-8 9-10	1-6 2-5 3-7 4-9 8-10
1-6 2-5 3-8 4-10 7-9	1-6 2-5 3-8 4-7 9-10	1-6 2-5 3-9 4-10 7-8	1-6 2-5 3-9 4-7 8-10	1-6 2-7 3-4 5-8 9-10
1-6 2-7 3-4 5-9 8-10	1-6 2-7 3-5 4-8 9-10	1-6 2-7 3-5 4-9 8-10	1-6 2-7 3-8 4-10 5-9	1-6 2-7 3-8 4-9 5-10
1-6 2-7 3-9 4-10 5-8	1-6 2-7 3-9 4-8 5-10	1-6 2-8 3-10 4-7 5-9	1-6 2-8 3-10 4-9 5-7	1-6 2-8 3-4 5-10 7-9
1-6 2-8 3-4 5-7 9-10	1-6 2-8 3-5 4-10 7-9	1-6 2-8 3-5 4-7 9-10	1-6 2-8 3-7 4-10 5-9	1-6 2-8 3-7 4-9 5-10
1-6 2-9 3-10 4-7 5-8	1-6 2-9 3-10 4-8 5-7	1-6 2-9 3-4 5-10 7-8	1-6 2-9 3-4 5-7 8-10	1-6 2-9 3-5 4-10 7-8
1-6 2-9 3-5 4-7 8-10	1-6 2-9 3-7 4-10 5-8	1-6 2-9 3-7 4-8 5-10	1-7 2-10 3-4 5-9 6-8	1-7 2-10 3-5 4-8 6-9
1-7 2-10 3-5 4-9 6-8	1-7 2-10 3-8 4-6 5-9	1-7 2-10 3-9 4-6 5-8	1-7 2-10 3-9 4-8 5-6	1-7 2-4 3-10 5-8 6-9
1-7 2-4 3-10 5-9 6-8	1-7 2-4 3-6 5-8 9-10	1-7 2-4 3-6 5-9 8-10	1-7 2-4 3-8 5-10 6-9	1-7 2-4 3-8 5-6 9-10
1-7 2-4 3-9 5-10 6-8	1-7 2-4 3-9 5-6 8-10	1-7 2-5 3-10 4-8 6-9	1-7 2-5 3-10 4-9 6-8	1-7 2-5 3-6 4-8 9-10
1-7 2-5 3-8 4-6 9-10	1-7 2-5 3-9 4-10 6-8	1-7 2-5 3-9 4-6 8-10	1-7 2-6 3-4 5-8 9-10	1-7 2-6 3-4 5-9 8-10
1-7 2-6 3-5 4-8 9-10	1-7 2-6 3-5 4-9 8-10	1-7 2-6 3-8 4-10 5-9	1-7 2-6 3-8 4-9 5-10	1-7 2-6 3-9 4-10 5-8
1-7 2-6 3-9 4-8 5-10	1-7 2-8 3-10 4-6 5-9	1-7 2-8 3-10 4-9 5-6	1-7 2-8 3-4 5-10 6-9	1-7 2-8 3-4 5-6 9-10
1-7 2-8 3-5 4-10 6-9	1-7 2-8 3-5 4-6 9-10	1-7 2-8 3-6 4-10 5-9	1-7 2-8 3-6 4-9 5-10	1-7 2-9 3-10 4-6 5-8
1-7 2-9 3-10 4-8 5-6	1-7 2-9 3-4 5-10 6-8	1-7 2-9 3-5 4-10 6-8	1-7 2-9 3-5 4-6 8-10	1-7 2-9 3-6 4-8 5-10
1-8 2-10 3-4 5-6 7-9	1-8 2-10 3-4 5-7 6-9	1-8 2-10 3-5 4-6 7-9	1-8 2-10 3-5 4-7 6-9	1-8 2-10 3-6 4-7 5-9
1-8 2-10 3-6 4-9 5-7	1-8 2-10 3-7 4-6 5-9	1-8 2-10 3-7 4-9 5-6	1-8 2-4 3-10 5-6 7-9	1-8 2-4 3-10 5-7 6-9
1-8 2-4 3-6 5-10 7-9	1-8 2-4 3-6 5-9 7-10	1-8 2-4 3-7 5-10 6-9	1-8 2-4 3-7 5-9 6-10	1-8 2-4 3-9 5-6 7-10
1-8 2-4 3-9 5-7 6-10	1-8 2-5 3-10 4-6 7-9	1-8 2-5 3-10 4-7 6-9	1-8 2-5 3-6 4-10 7-9	1-8 2-5 3-6 4-9 7-10
1-8 2-5 3-7 4-10 6-9	1-8 2-5 3-7 4-9 6-10	1-8 2-5 3-9 4-6 7-10	1-8 2-5 3-9 4-7 6-10	1-8 2-6 3-10 4-7 5-9
1-8 2-6 3-10 4-9 5-7	1-8 2-6 3-4 5-10 7-9	1-8 2-6 3-4 5-9 7-10	1-8 2-6 3-5 4-10 7-9	1-8 2-6 3-5 4-9 7-10
1-8 2-6 3-9 4-10 5-7	1-8 2-6 3-9 4-7 5-10	1-8 2-7 3-10 4-6 5-9	1-8 2-7 3-10 4-9 5-6	1-8 2-7 3-4 5-10 6-9
1-8 2-7 3-4 5-9 6-10	1-8 2-7 3-5 4-10 6-9	1-8 2-7 3-5 4-9 6-10	1-8 2-7 3-9 4-10 5-6	1-8 2-7 3-9 4-6 5-10
1-8 2-9 3-4 5-6 7-10	1-8 2-9 3-4 5-7 6-10	1-8 2-9 3-5 4-6 7-10	1-8 2-9 3-5 4-7 6-10	1-8 2-9 3-6 4-10 5-7
1-8 2-9 3-6 4-7 5-10	1-8 2-9 3-7 4-10 5-6	1-8 2-9 3-7 4-6 5-10	1-9 2-10 3-4 5-7 6-8	1-9 2-10 3-5 4-6 7-8
1-9 2-10 3-5 4-7 6-8	1-9 2-10 3-6 4-8 5-7	1-9 2-10 3-7 4-6 5-8	1-9 2-10 3-7 4-8 5-6	1-9 2-4 3-10 5-6 7-8
1-9 2-4 3-10 5-7 6-8	1-9 2-4 3-6 5-10 7-8	1-9 2-4 3-6 5-8 7-10	1-9 2-4 3-7 5-10 6-8	1-9 2-4 3-7 5-8 6-10
1-9 2-4 3-8 5-6 7-10	1-9 2-4 3-8 5-7 6-10	1-9 2-5 3-10 4-6 7-8	1-9 2-5 3-10 4-7 6-8	1-9 2-5 3-6 4-8 7-10
1-9 2-5 3-7 4-10 6-8	1-9 2-5 3-7 4-8 6-10	1-9 2-5 3-8 4-6 7-10	1-9 2-6 3-10 4-7 5-8	1-9 2-6 3-10 4-8 5-7
1-9 2-6 3-4 5-10 7-8	1-9 2-6 3-4 5-8 7-10	1-9 2-6 3-5 4-10 7-8	1-9 2-6 3-5 4-8 7-10	1-9 2-6 3-8 4-10 5-7
1-9 2-6 3-8 4-7 5-10	1-9 2-7 3-10 4-6 5-8	1-9 2-7 3-10 4-8 5-6	1-9 2-7 3-4 5-10 6-8	1-9 2-7 3-5 4-10 6-8
1-9 2-7 3-5 4-8 6-10	1-9 2-7 3-8 4-6 5-10	1-9 2-8 3-4 5-6 7-10	1-9 2-8 3-4 5-7 6-10	1-9 2-8 3-5 4-6 7-10
1-9 2-8 3-5 4-7 6-10	1-9 2-8 3-6 4-10 5-7	1-9 2-8 3-6 4-7 5-10	1-9 2-8 3-7 4-10 5-6	1-9 2-8 3-7 4-6 5-10

Table 184.3: Acceptable permutation-circuit wirings for the T52 versions A, B, and D.

Versions A and B

The first two versions of the machine differed only superficially; their operation was identical. They contain no new elements beyond what we have already discussed. The machine is initialized by putting the ten wheels into the positions specified by part of the key. The output of each wheel is assigned to control a bit-flipping (XOR) or a bit-swapping (one of the relays) via a plugboard; this mapping is another part of the key. After each character is encrypted, all ten wheels advance (rotate) their positions by one; this is what we call "regular stepping." A schematic diagram of the T52a/b is in Figure 184.4.

To specify the key, we need to give the assignments and starting positions of the ten wheels. The names of the wheels are implied, so if we write the key as

9-10, 1-6, I, II, 3-5, 4-7, IV, 2-8, III, V; 52, 19, 21, 50, 47, 24, 14, 46, 39, 7

we mean that wheel A starts at position 52 and is assigned to a swapping relay that is connected to points 9 and 10 (see Figure 184.2), wheel B starts at 19 and is assigned to a swapping relay between points 1 and 6. wheel C starts at 21 and is assigned to the XOR on data line 1, etc.

Let's see how to translate between the language in which the key is expressed into a set of operations on the data bits. For the example above, we see that the XOR operations are controlled by the output of wheels C, D, J, G, K. To glean which bits are swapped in the permutation circuit, we can shift things in Figure 184.2 so that points connected to the same relay are in the same vertical segment, as seen in Figure 184.3. From this we see that wheel B controls a transposition (1 3), which occurs first (if it occurs, based on the output of B). It is followed by (2 5) which is controlled by H, then (3 4) controlled by F, (4 5) controlled by E, and finally (1 2) controlled by A.

To see that we understand the machine and that your implementation of it is working, consider the following test vector. Encode the first line of Hamlet's soliloquy in Baudot:

```
TO9BE9OR9NOT9TO9BE+N89THAT9IS9THE9QUESTION+C843
```

Encrypt with T52a/b using the example key to get

```
9NQHMTA9XYJDYSFVUOAZ9/YEIW/8GX84RAURJSRA/9KOMH9
```

The encryption of the first letter goes as follows. The wheels are in their initial positions, so A's output is 0, B 0, C 0, D 0, E 1, F 0, G 1, H 1, J 0, K 1. The first character is `T`, which has bits 00001. Its first bit is XORed with 0 (the output of C) to remain 0. The second bit is XORed with 0 (output of D) to remain 0. The third is XORed with 0 (output of J) to remain 0. The fourth is XORed with 1 (output of G) to become 1. The last is XORed with 1 (output of K) to become 0. After the XOR circuitry, the data lines carry the bits 00010. The output of B is 0, so the first transposition occurs, and bits 1 and 3 are swapped (no effect). H outputs 1, so its transposition does not occur. Because F outputs 0, the transpositions (3 4) does occur and now we have 00100 on the data lines. The output of wheel E is 1, so its transposition does not occur. The last transposition, (1 2) occurs, but it swaps two zero bits. The output of the machine is therefore 00100, which is written as `9` in Bletchley notation and which represents a space.

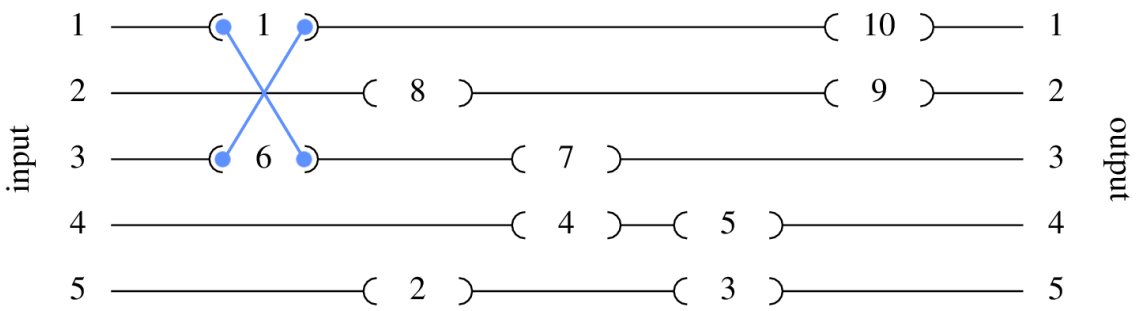

Figure 184.3: Example of shifting the access points in the permutation circuit so that we can glean the transpositions. Note that access points cannot be shifted through one another.

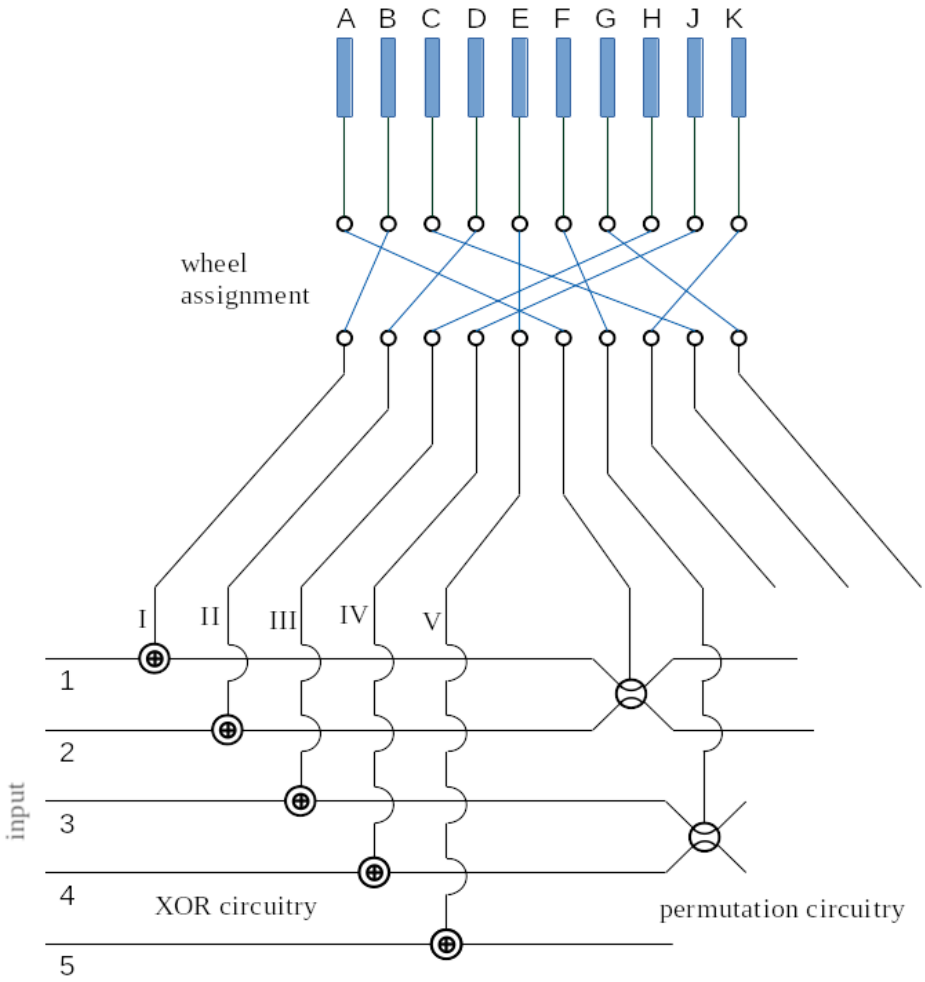

Figure 184.4: Schematic diagram of the T52a/b. The diagram is incomplete; only two transpositions are shown in the permutation circuitry.

Version C

Version C has the following changes from versions A and B:

- Between the wheels and the wheel-assignment plugboard is a set of switches for setting a message key and circuitry to shuffle the signals on the control lines from the wheels. When too many messages are sent with the same daily key, it is easy for analysts to reconstruct the plaintexts. Modifying the key for each message obviates this problem.
- After the control lines leave the wheel-assignment plugboard, they pass through what is called the "SR logic" module which uses XOR circuits to further scramble them.
- The permutation circuitry is fixed so that only the wiring 1-2, 3-4, 5-6, 7-8, 9-10 is used. The corresponding transpositions (in order) are (1 5), (4 5), (3 4), (2 3), (1 2). Because only one configuration of the permutation circuitry is used, the connections are renamed with abbreviated labels: "1" for 1-2, "3" for 3-4, "5" for 5-6, "7" for 7-8, and "9" for 9-10.

The message-key unit has five switches, each of which can be set to positions labeled `P`, `S`, `T`, `U`, `W`, `X`, `Y`, and `Z`. Each switch's position activates up to three transposition relays that can swap the signals on the control lines leaving the wheels; see Table 184.4. The transposition relays are placed into three layers, so that layer 1 acts before layer 2, which acts before layer 3; see Table 184.5 for the transpositions and their placements into the three layers. It goes without saying that the action of the message-key unit and the wheel-assignment plugboard together are like using the plugboard with a new set of assignments; the addition of the message-key unit does not change the T52 in a fundamental way.

As an example of the function of the message-key unit, consider message key `WUPSY`. Switch 1 is in position `W`, which means that transpositions T01 and T06 are active. Switch 2 is in position `U`, so T02 and T07 are active. Switch 3 activates T03. Switch 4 activates T09 and T14. Switch 5 activates T05 and T15. In the first layer of transposition relays, T01, T02, T03, and T05 are active. From Table 184.5 we see that the control signals from wheels A and B are swapped, from C and D are swapped, from E and F are swapped, and from J and K are swapped. In other words, line B now carries the signal from wheel A, line A now carries the signal from wheel B, etc. In the second layer, T06, T07, and T09 are active. So the signals on lines B and C are swapped, D and E are swapped, and H and J are swapped. In layer 3, T14 and T15 are active, and they swap the signals on lines D and J, and E and K. The overall permutation enacted by the message-key unit in our example takes the signal from wheel A and puts it onto line C, the signal from wheel B onto line A, etc.:

A	B	C	D	E	F	G	H	J	K
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
C	A	J	B	F	K	G	D	E	H

switch number	transpositions (swappings)	switch positions P	S	T	U	W	X	Y	Z
1	T01				✓	✓	✓		✓
	T06		✓			✓		✓	✓
	T11			✓			✓	✓	✓
2	T02			✓	✓	✓		✓	
	T07	✓			✓		✓	✓	
	T12		✓			✓	✓	✓	
3	T03	✓	✓	✓		✓			
	T08		✓		✓	✓		✓	
	T13			✓	✓	✓			✓
4	T04	✓		✓				✓	✓
	T09		✓	✓		✓			✓
	T14	✓	✓	✓			✓		
5	T05	✓				✓	✓	✓	
	T10	✓		✓			✓		✓
	T15	✓			✓			✓	✓

Table 184.4: Switches in the message-key unit. Each of the five switches can be set to one of P, S, T, U, W, X, Y, Z. *The effect of each switch is to activate up to three swappings (transpositions) of the control signals from the wheels* A, ..., K. *See Table 184.5 for the action of the transpositions.*

transposition number	layer	control wires affected
T01	1	A B
T02	1	C D
T03	1	E F
T04	1	G H
T05	1	J K
T06	2	B C
T07	2	D E
T08	2	F G
T09	2	H J
T10	2	A K
T11	3	A F
T12	3	B G
T13	3	C H
T14	3	D J
T15	3	E K

Table 184.5: Transpositions in the message-key unit. Transpositions that are active in layer 1 occur before layer 2, which occur before layer 3. If a transposition is active, then it swaps the signals on the designated control lines.

output	inputs									
	I	II	III	IV	V	1	3	5	7	9
I		X		X				X	X	
II			X		X		X	X		
III		X			X	X	X			
IV	X		X			X				X
V	X			X					X	X
1	X		X			X	X			
3		X		X			X	X		
5			X		X			X	X	
7	X			X					X	X
9		X			X	X				X

Table 184.6: SR logic for version C. Each output line carries the XOR *of four input lines.*

The wheel-assignment plugboard maps the control lines A, ..., K to ten lines labeled I, II, III, IV, V, 1, 3, 5, 7, and 9. These labels reflect their rôles in controlling the XOR and permutation circuitry. But before they carry out those rôles, they pass through the SR-logic unit. Each of the outputs of this unit is the XOR of four of the inputs; see Table 184.6 for the assignments of the inputs to outputs.

The key for T52c consists of the settings of the wheel-assignment plugboard (with the abbreviated labels for permutation relays), the initial wheel positions, and the message key. For example:

9, 1, I, II, 3, 7, IV, 5, III, V; 52, 19, 21, 50, 47, 24, 14, 46, 39, 7; `WUPSY`

With this key, the first line of Hamlet's soliloquy is encrypted to

```
FAYUMGR+UHOEC8/8BB+STFJKAMWX/GPZJMLGUZJZZV/JJ9G
```

Version CA

Version CA is identical to version C with one exception: the SR-logic circuitry is changed (see Table 184.7) to reduce some vulnerabilities.

With the same key and plaintext as in our example for version C, the ciphertext for version CA becomes

```
E9VNT9BJL9GFXMMM+/CO/JG9CYNGL9RBDHPJA4BDDSJP99O
```

output	inputs									
	I	II	III	IV	V	1	3	5	7	9
I		X			X	X	X			
II	X	X	X	X						
III				X			X	X		X
IV	X		X					X	X	
V			X		X		X	X		
1	X			X					X	X
3						X	X	X	X	
5	X	X			X				X	
7		X		X		X				X
9			X		X	X				X

Table 184.7: SR logic for version CA. Each output line carries the XOR *of four input lines.*

Version D

Version D has the same features as A and B, with one addition: irregular stepping of the wheels. For each wheel, a pin is tapped at a specific offset further ahead of its current position (offsets are given in Table 184.8). The outputs of those taps are carried on ten new control lines, labeled a, b, ..., k. An eleventh control line carries the middle bit (bit 3) of the previous plaintext character and is labeled z. Whether the eleventh control line is used depends on the setting of a switch on the machine, called the "klartext feature" or "KTF" ("klartext" simply means "plaintext"), and which is set to ON or OFF. Whenever a control line is active, we say that it carries a 1 or TRUE; when inactive, a 0 or FALSE. Whether a wheel advances to the next position (steps) depends on the evaluation of a logical expression involving the truth values of the control lines. What that expression is also depends on whether the KTF is in use. See Table 184.9 for the expressions for each wheel for each KTF setting.

The key of the T52 version D resembles the key for version A/B, with the addition of the KTF setting. For example, if we take the key we used for version A/B, and set KTF off, the key is

9-10, 1-6, I, II, 3-5, 4-7, IV, 2-8, III, V; 52, 19, 21, 50, 47, 24, 14, 46, 39, 7; OFF

and the first line of Hamlet's soliloquy is encrypted to

```
9983TW+WDHYV8V+8WVOJCOZSERDSU++QBXPVAR3LF+4PD8F
```

When the KTF feature is used and the key is

9-10, 1-6, I, II, 3-5, 4-7, IV, 2-8, III, V; 52, 19, 21, 50, 47, 24, 14, 46, 39, 7; ON

the ciphertext is

```
9989NAK43O4GQYQ8CMZVZUQZOHTAB+3FVYOR9+3LIU9CZVB
```

wheel	stepping-pin offset
A	25
B	24
C	23
D	23
E	22
F	22
G	20
H	20
J	18
K	16

Table 184.8: Offsets for the pins controlling irregular stepping. The pin whose signal helps to control irregular stepping is the given number of places beyond the current position of the wheel (modulo the size of the wheel).

wheel	logical expression when KTF=OFF	logical expression when KTF=ON
A	(NOT e) OR (NOT f)	b OR c OR z
B		(NOT c) OR d OR z
C		(NOT d) OR e
D		(NOT e) OR (NOT f)
E	f OR (NOT g)	f OR (NOT g) OR (NOT z)
F	g OR h	g OR h OR (NOT z)
G	(NOT h) OR (NOT j)	
H	j OR (NOT k)	
J	(NOT a) OR k	
K	(NOT d) OR e	a OR (NOT b)

Table 184.9: Logic of the irregular stepping in versions D and E. A wheel steps if the required logical expression evaluates to 1=TRUE*. The logical expression depends on whether the klartext feature is* ON *or* OFF*. The variables in the logical expressions are the outputs of the pin from the corresponding wheel (“*a*” for wheel* A*, etc.) at an offset given in Table 184.9. The variable* z *is the middle bit (bit 3) of the previous plaintext character. Variables carry the values* 0=FALSE *or* 1=TRUE*. The* NOT *operation flips a bit (*0↔1*). See Table 184.2 for a definition of the* OR *operation.*

Version E

Version E resembles versions C and CA, with these changes:

- The message-key unit is not present.
- The SR logic is changed. See Table 184.10.
- Irregular wheel stepping (including the KTF) is added in the same way as in version D.

The key is specified as it was for versions C and CA, with the modification that the message key is replaced by the KTF setting. For example, using the key

9, 1, I, II, 3, 7, IV, 5, III, V; 52, 19, 21, 50, 47, 24, 14, 46, 39, 7; OFF

we encrypt the first line of Hamlet's soliloquy to

```
SVPWX9PT3ULW3TFMKE3KC4N9CPNESJSJXVTVJ/SGOOJGIPI
```

With the key

9, 1, I, II, 3, 7, IV, 5, III, V; 52, 19, 21, 50, 47, 24, 14, 46, 39, 7; ON

we get

```
SVP4AV9TZWPMZRTEMQQQBYI3WAVQ+NTECMX/IHSX8/WCQTR
```

output	inputs									
	I	II	III	IV	V	1	3	5	7	9
I		X		X				X	X	
II					X		X	X		X
III	X			X		X	X			
IV	X		X		X					X
V	X			X					X	X
1			X		X	X	X			
3	X	X	X	X						
5			X		X			X	X	
7		X				X	X	X		
9		X				X			X	X

Table 184.10: SR logic for version E. Each output line carries the XOR *of four input lines.*

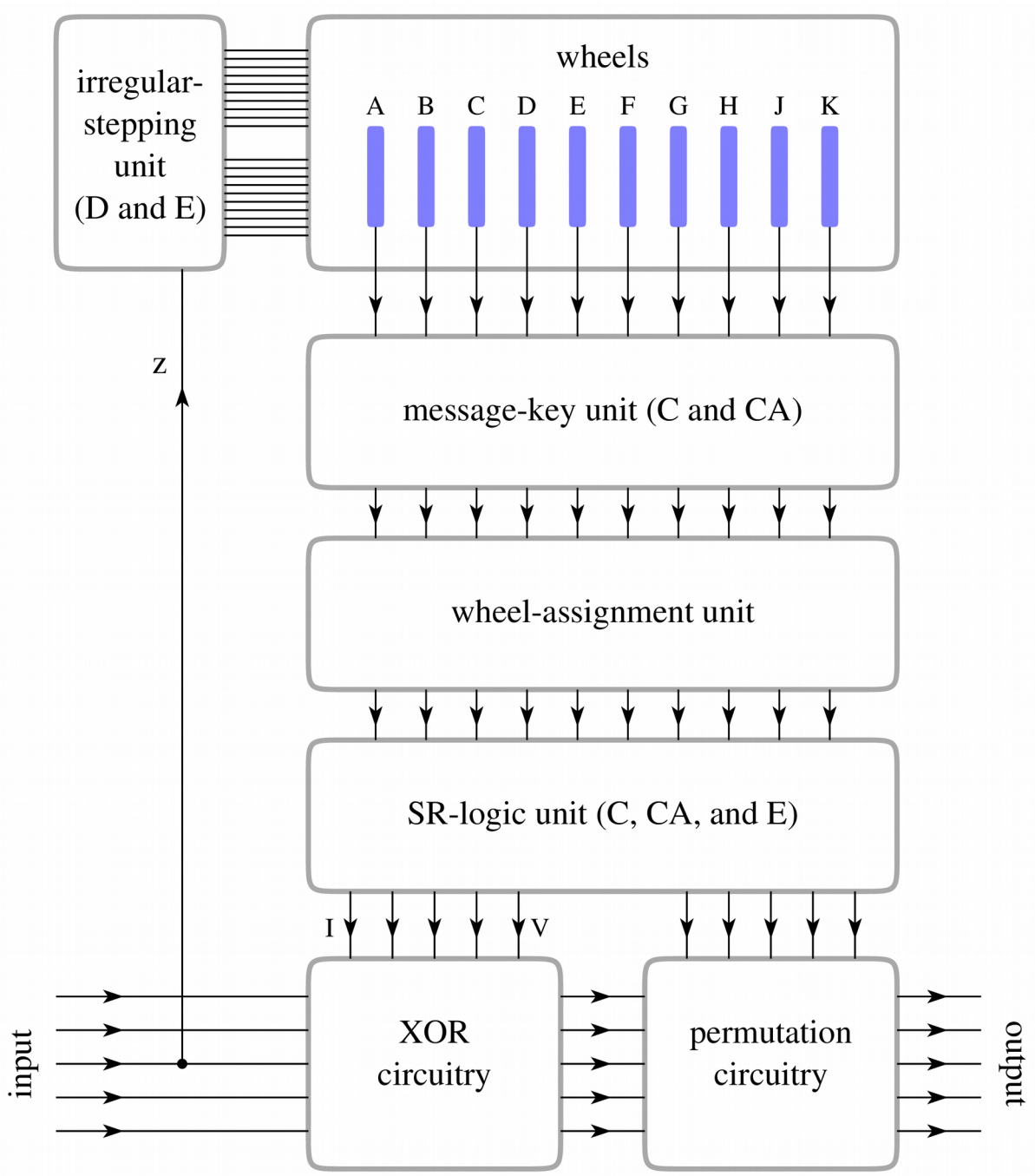

Figure 184.5: Overview of the T52. Each module is labeled according to which versions of the machine it appears in. All versions have the ten wheels. From them come ten control lines, A, ..., K. In versions C and CA, the control wires pass through the message-key unit which shuffles their signals; in other versions the control lines run directly to the wheel-assignment module, which is present in all models and which also shuffles the signals. In versions C, CA, and E, the control wires enter the SR-logic module which modify the signals in such a way that each output depends on four of the inputs. Five control lines actuate XOR *operations in the XOR module, while the other five control the permutation module. In versions D and E, there is an irregular-stepping-control module. It takes signals from the wheels and plaintext to determine which wheels advance.*

Reading and references

Frode Weierud, “Bletchley Park’s Sturgeon, the Fish That Laid No Eggs,” *The Rutherford Journal: The New Zealand Journal for the History and Philosophy of Science and Technology* 1 (2005-2006), https://www.rutherfordjournal.org/article010106.html (Figure 2 of this document has errors)

George Lasry, “T52 Functional Description.” This document can be found in the supplementary materials for some challenges on MysteryTwister, in this zip file:
https://mysterytwister.org/media/challenges/add/mtc3-lasry-T52-add.zip

George Lasry, “T52 Cryptanalysis.” This document can be found in the supplementary materials for some challenges on MysteryTwister, in this zip file:
https://mysterytwister.org/media/challenges/add/mtc3-lasry-T52-add.zip

Donald W. Davies, “The Early Models of the Siemens and Halske T52 Cipher Machine,” *Cryptologia* 7:3 (1983) 235-253, https://doi.org/10.1080/0161-118391857964

Donald W. Davies, “The Siemens and Halske T52e Cipher Machine,” *Cryptologia* 6:4 (1982) 289-308, https://doi.org/10.1080/0161-118291857118

Donald W. Davies, “New Information on the History of the Siemens and Halske T52 Cipher Machines,” *Cryptologia* 18:2 (1994) 141-146, https://doi.org/10.1080/0161-119491882801

Wolfgang W. Mache, “The Geheimschreiber,” *Cryptologia* 10:4 (1986) 230-242, https://doi.org/10.1080/0161-118691861065

Wolfgang W. Mache, “The Siemens Cipher Teletype in the History of Telecommunications,” *Cryptologia* 13:2 (1989) 97-117, https://doi.org/10.1080/0161-118991863817

David Kahn, “The Geheimschreiber,” *Cryptologia* 3:4 (1979) 210-214, https://doi.org/10.1080/0161-117991854089

Crypto Museum, “T-52 Geheimschreiber: Teleprinter cipher machine (STURGEON),” https://www.cryptomuseum.com/crypto/siemens/t52/index.htm

Programming tasks

1. Simulate the T52. Include a switch to determine the version (A/B, C, CA, D, E). For versions A, B, and D, include a function that checks that a permutation-circuit wiring is acceptable (there may be ways of doing this without using a look-up table).

2. Develop a brute-force attack for a situation in which the wheel assignments are known and some of the wheel positions are known. It may be faster to use the index of coincidence to reject most decryptions, and the fitness as a second stage of verification. Using a faster, lower-level language (such as C) would also be a benefit.

3. Develop a hill-climbing attack that maximizes the index of coincidence if the wheel assignments are known but their positions are not. This is not likely to work for versions D and E.

Exercises

1. Decrypt this ciphertext with version A/B and the given key.

   1-4, 2-5, IV, I, II, 3-9, 6-8, 7-10, III, V; 43, 45, 15, 67, 50, 35, 22, 29, 39, 42

   ```
   RJLQHMILUAMODRT8LX8IYVFYW4WPB9WUW/VWCNKPXW/R3F+AA3F9EZGLNJABW8KP
   IT/IRP3NKHEACWGBJ4W9DN8/NEH/T+XHT+WKPURIDTH8YV++JHACHXUMZTHUIAGI
   OPCTPTFOQDWK3ZSSAF883AEGI+RIT/XWRTNEM4DN9KBW+IJCMXO9RKBUTANRYZ4D
   YV+W3XBBUPM8EOS/HG9DYE+RE+J/WHRV8VKA/W8MQ+89Y8PR9RHJ9QDQVUY3EBTZ
   XJLXZN4WZYSOMHSV3NOD+WU4HPR/UWWOTQS+YEVPJRUFUT84ZU4HTCUF8LE/RWEJ
   3WCY4WULXTB/MLE3EG
   ```

2. Decrypt this ciphertext with version C and the given key.

   II, 5, V, 1, I, III, 3, 7, 9, IV; 53, 65, 32, 5, 42, 56, 38, 42, 29, 38; WXPSY

   ```
   4S8/9ZXBINQY+DO3ZEOYBFXAOYDRG9KCTRD9PFJSIJMU+EIDWJUQZYKKW+S8BV3E
   +FNYWXOMUUBZVSYVSKSJLHLY+ZRDPDMWDFWLIBPOC4CNXME9IIMO+PBAACFS+GU3
   YSSG9NEYPFS8QB/DYFNM9KV+3MYYH3MR4R3B+PUBFDKEVBFOGVZFQ4/8QTRPEMRJ
   OROSCM4+TG4ANYMKAQ9KSTMDRXCXFWFSY/TMXG8V+/U3C+T9H3DHZVHW3JHD343R
   ILJLCR4RYETNSTW9VT9U3BPXDA/NGF
   ```

3. Decrypt this ciphertext with version CA and the given key.

   1, 5, V, III, I, IV, II, 9, 3, 7; 53, 17, 56, 31, 65, 30, 44, 57, 24, 32; PZSXZ

   ```
   9O8+KIVIASQEWPBPARL4VCGI9FW4/YCNZK/RCMSOX+ZVCGDFU4O+/FMDLSU3W/8D
   EWK88CG/G94FD8NRDVLCFXYO/EOPEII3CESZMNNIHU83TMUZ//AIMSBMPYONZPVJ
   9PWTFZDEJIOSTY+PEANV+PGVDKOYK/CMT9HE8+CHH//CKSLQVGJOH+BQDP+BNVAF
   MK8LWVA3DLP/YI9/O93HYYVUC4S9E4KECDAQXURZUOCFCE9SR9WKHACIF3DMNCH3
   X9Z+C/EN44L4GW8
   ```

4. Decrypt this ciphertext with version D and the given key.

   2-5, 7-10, II, 3-6, III, V, 4-8, IV, I, 1-9; 46, 7, 30, 52, 51, 10, 60, 33, 21, 8; OFF

   ```
   R/XJY3AB+MYJ/344VCJHW8GHTF8QFTVAOXCG9MDH8FMR9+YWBQOPYEFV3D94BUQT
   FB8B394FS33DMBC4+KAU93UP+UAQ4QTUMFGFURDIYT+4ISLVKWVKTELTNIME3L/H
   Z8SXJNHOMOQFIITEHWG8ZPD+D4N/TLJ+/FRPO8MI/J4I8TB+URQBPV+4V3STNPFO
   LE/L+WH/3NZ9HK8WPOWXUS9SODIOPR3+SCNZ9H3OM+WJ8CCGA4LBDZU4+38SKATI
   IKE4FK4BOEST9HVQ4VKBGAD3DW8MX/UMTIOS/PUURDBZGEMG+NA/XQC8/MHLGIUR
   OAXSRBZ+RJ3ADO/M/SPRY4CKGODFUASTVE+LAJOMHRVPBVMDX494+/PCSZINQJCM
   EJKDCQT/RCRICUG9XBSXEQO4KUMMKNMX4+PPYV/QPYYPI9LFZ+OMQWSJP9VZBP8I
   ASZ+/9IUZZ+H9+W8MGMQPH4YX4ROK4NR4+SAJLRQXZKQTZCGJCZFN+APELPAL8N8
   IS
   ```

5. Decrypt this ciphertext with version E and the given key.

   III, 9, IV, 5, 1, II, I, 7, 3, V; 56, 32, 59, 59, 11, 27, 29, 10, 52, 41; ON

```
RAZIGAH+ESFJD4G/S8HOWUSQ9ZSKDZOR9WATHMEAV/RBDQDJWYYBRCDUHSOTS
YNVT4/HJWWMIVLDFIPXKOPMZD9CHSRINYSDXYHVBRKUHCRQZQQL/VDOGUBSA+
BHKDWRP8EAL8KJXYA8/KSJD9KRP4HPH9EPE/N9ZLGTRT9GEG+NSNPY39KZVNP
9ABPTDS9GCEEKVFIQW
```

6. The following ciphertext was encrypted with a T52a/b. The wheel assignments and half of the initial wheel positions are known. Brute-force the remaining wheel positions and decrypt the text.

   wheel assignments: A IV, B I, C 6-9, D 8-10, E 2-4, F III, G 1-5, H V, J 3-7, K II
   wheel positions: A 11, B 27, C 4, D 15, E 48

```
+3RAYZQMHNJWFF8N8OFESRUYUTM/4VKONQK8RCTNA4TTMTQ3TYZKMDEFWK3/NNKI
MCICDEK+OWDVHOE9DERPYV3DHS4+LC/MR4SCJBWUISWKMZM8TCOX/E+FJHRCFM8U
XTNTTPJF49QOEZISIJWNHOGIC8CAWOUCD3/YFW84LENYTNI+H9BBOLJBQRQLDAVP
N+A/BCMO4WTJ4PVSWPP4MS8UJVYP3LLPDJNGEBUZ9AT3HRHO/OCQ8KGS+UILYYYY
+CKYCEKGHELMAFYSJTVH/ZWDW8EOHB+IE3YS8LAHSETWP3CJAKYKP9O9M9ZCOR
```

   This exercise is similar to a challenge from MysteryTwister (https://mysterytwister.org), which can be found at https://mysterytwister.org/media/challenges/pdf/mtc3-lasry-14-T52-01-en.pdf.

7. The following ciphertext was encrypted with a T52c. The wheel assignments and half of the initial wheel positions are known, as is the message key. Brute-force the remaining wheel positions and decrypt the text.

   wheel assignments: A 7, B 9, C IV, D II, E V, F 1, G III, H 5, J I, K 3
   wheel positions: A 33, B 52, C 34, D 4, E 9
   message key: ZXYYS

```
G/PBVQSM9YLM+E4HKUXFPN4+GGCVKNRMDBRX3JLKI4+JDEGF+DT4RO9RDS8NWZLY
TZG+LM44V9TVXYMZTYW99LEHT3NVOJNARQ9T9FIO/XKLS8KM98OIRPMM9+GH/WP8
+Q/GEWQU9XXWJDCQ83W/3ZNZM/YM+AFWLY8JXH+YBMMQ4QHX+PERX+FNMSF/F9JZ
C/X8UDXNB+J8CSSMEIYLB4+TMXZPBG+LAOHSPFENHPA3/CZ4I9LSWDFJOBRJEA8C
8FPGROMGWS4SGCD9YLVTJGNG+ABFGXFVI+9KIC/M8EMQBZWSLP99STHU3AYC/VCB
YWUGNO9M/MUFQGZIK9Q99+OTU8HEFDA+MWJD9FQU9+CIBNEUKXXP34POB3CMD4Y/
UDWBIPUNLCFPNYT/AQPOQ9IKI98JKF9DCR+9/OES89MCEYP+SCNEQIR8YHOLYGJM
NJB+XNHV4TV4DLKSS8PTNOM/DJTZESIKWYJOF3U4SGFIO8M4VUYOSPF+IXXZXBW3
RQS38
```

   This exercise is similar to a challenge from MysteryTwister (https://mysterytwister.org), which can be found at https://mysterytwister.org/media/challenges/pdf/mtc3-lasry-15-T52-02-en.pdf.

8. The following ciphertext was encrypted with a T52d. The wheel assignments and half of the initial wheel positions are known, as is the KTF setting. Brute-force the remaining wheel positions and decrypt the text.

   wheel assignments: A II, B I, C 4-6, D 9-10, E V, F 3-7, G 5-8, H III, J 1-2, K IV
   wheel positions: A 1, B 43, C 6, D 62, E 2
   KTF : ON

```
B9JCH4CCDNHCJ83JXHCNG+GM+NLYIBFRNOV9BEWLAB+QDOT3DHJQUHEXHJJ+/HYO
KPZ3SZP9C+X3M98J9JOWB/GZLMEUXVDWYNF8ZC9OVYYCLALAQVS/8V9XVUKDEWMQ
```

```
JVT3O/BXSDRZXCN/GSH3E+DPALBSVCSUV+XP9N9APFJL3LGDGP+B4++SQLUJGFMW
3ZKGIHWRWRN+TQTM9WNGSM93UFB+ZVHOBUBA3YMUJGBAPC9IGYGMJZ+WFXR4E9ZP
POYQ9CTPL9XGOIESCGGX+XRMBYWTVPYQB3R4MYXJFZTGN8TJ/W/UNNY/IUY98YAS
KISW/CPWC/RYAWTKE3VFWG/PSUZ/4V4AR9CMQLFXPJ8MULXB4H8NTVKYU+JXZDT8
ZQR+8CQQRODGJJH/KFTTW/DLQF+FCMLJTTPRUTPLYZQDA+EQ4R/3DCA+IY34LD8H
+EBYSYOSHRSP39
```

This exercise is similar to a challenge from MysteryTwister (https://mysterytwister.org), which can be found at https://mysterytwister.org/media/challenges/pdf/mtc3-lasry-16-T52-03-en.pdf.

9. Below is a ciphertext in Bletchley Baudot notation. It was encrypted with a T52 version A or B. Part of the key is known:

    wheel assignments: A 4-9, B III, C IV, D 3-6, E V, F I, G II, H 1-7, J 2-8, K 5-10

    Use your hill-climbing attack to find the wheel positions and decrypt the text.

```
XOYDGSTFC9EN8QVGMADUIHYXBQARRML+/YDQP8KCR93SF+G8WQ+EQKU/33V8XHIK
HUU9F3YQWXJLJO/BKQ9M+SOETV/FA8L83CSR//CIIW+E8XNNAPC8J+LBQLJ/8UTR
HFZOB3QT/PA+M4V/K3FIQBG8/MLEJ8R/4FZLEOIX9+3LF/F8VVMBP3GQG4NPRTZP
ZMDDKGDWHL3F+LLCBPSBJFC/B8TYB4CZ/NTBHRMJO/JDXAEJUK/UIT8CO4MN+ILK
BNU/NFDMIIJ/XKJYY3YKCN8YIFKVEE9UUFHXI9FNNQ++FTOKFUMYD/B8DHCICAYQ
NJLZESKWQJ+MRY8GRMWWDJESVTVC/PFMMMZFO8J3/ORSAIG9LDJZBOMDEIX3QMRI
83IF+TLYWUELHMAGOSPMMIT3YJ/XTQQYGN4G8HTBNWFGHNBR9JH+FUC3PXFHBAEV
QQ3ITBMOHY9NGWQXPTNKB/GCL3XRSCUR3HR4X8QPP4BTD3VI4SATOJNJIKNAUHF/
FSJZIO+ETSWEMF84M3DMIBESKD8LY88BARJNMBAX8HOYYAFQYBK9GQHXPCGXILRL
34SCJ9REJRKZQRGIYRYRQEK8RPPQUKNKGALWKM+PAOWGJ4NK9GWKPDDYKX3SMCBC
OL99MRTTGWZ/KSZVZGGGQX9TDT+BBW4PABVFFKFIMLMZVQY+F/GHA+YC+8J3YS+M
RL/XPOJA+8OJWRBZ/9SQ/XG8QGLRHAMI/GANR9BQDDGJ3RCXR+9DKE4UMPT8HXAM
SMNSX/FZTOSI33QFA+J+QMVAI4ZX+H3GO9YTLRF/PY3ZURW+DRLGA3UG/+IOHTMG
BYLL9LCOJI3M/QKJFHAQEDT8RVTCLKISTVIGF3XAIBBNMSRCDWBG9FXJDDKWVDTQ
/98VQTQT3N4M8IGYXKN+B3CXEH+EWK8TAKIJU9+3DVOPVZEOIYBARD
```

This exercise is similar to a challenge from MysteryTwister (https://mysterytwister.org), which can be found at https://mysterytwister.org/media/challenges/pdf/mtc3-lasry-17-T52-04-en.pdf.

10. The broken T52a: Imagine a T52 version A that is broken so that its transposition relays stick and the permutation that it uses is set by the initial configuration of the machine and does not change as a text is encrypted. Find a way to break this ciphertext that was produced by the broken machine:

```
/PGU9VJYZJROE3T9398VEE8XJPT+ICVESQ44XJIDDB8EKZCUEBLS+JRZ/T3HGWU+
8NNUDKUQLPOMXUS/AOOSBRWW3W3PKFDUQQQE+S3CZW9FFE4SEOHWBGLQO9XOOHMQ
LMRNLKQDFEORUDL8W/DGIWZVJ98GMUNBQO4MX8B3F+8RD9CCQHUKKI3CNZ+RKVFA
+AGFULBDCOD/GZ/3AXY9/WG+TVM/TLMI3SD9HDN9FWX4DT/W9KLFDCWOPAITUL/4
B+CXQBSMB+3AWASW+ES4JBYQBXKMTDWOF+/+PJYE+MS84FSJ4GW84YLRVOM+4PCZ
D8UAXP8XXFFORMRMJHLVSIMSXQSNCPQFCYGCX+4QF/W9+BDWQW+ZVQRULCRPOZGQ
RE/4EPZRLUWJ8IIK8QU3ZKSKN/H3WSGG98EGT4LDH4Q4BF+JE3I+4C9MZ9SZ9NP3
E+LT88JYWYODU9EH+9CZAWHODMLWV/JWFQPEPBAZBG+O8QYKN4//YKJWTLYI+NTA
S9IS4F+HE+OP8COJ8IDI+8JQ8NYFPX+AZCVM+Q/OPBZ+8FLJWKPVWPTIU3X9D/V8
OI9WO4S/YE43Y93M+MWDXT+ZFBLQJJ44J/+FP9NSQ3W8UJY+FZ4+FL9CO+E88MSQ
+JLVDOJGJTKJ+M8SAIWPOCXAYCLVDBK8O/VG9LC8OG/PDAH+WN/3P8HEY8+KHI/A
```

```
8Y3NEWBUAVG+UKXHU9FIPPBAIOURYFWUANA+BX3IWOOUKZCPYAHMKTG3OJOIR3L+
BQGLE+XDIRQTC3JEYHZ9RAHW4CM3PJ4DQYSV8XUE3X8MEFMW9NQSNBFMTDS4UOLK
VEKKNXQ8A/IQXHKCFTDSQ/ANREIVIBQA+CK3EQMX4QFEZYZ8ZT8EYSW9/WSQOJRO
Q8PQAX3MSA9TDZBAUWLNRJIX4RBHPK/EJLUVBBV8U3EW9XFUNVS83SCLNP8FAO4Q
QSNDEQW4QNYCERWF8AAYUT+HQ9RVPY3OO49VBW8YTRYAIBKJMPJUAEHPOXQPC/VV
K3TQA/UXPHJHT9GN83+HXTDUHQPVJ84RB+VMZBQ+O9QXAEODXL/QSG/PLEIZTWHM
+NIMJTJ8A3VIRJ8/XFJ98ZRSYJI+4R//ZCAYO83ADNXQZF3EINPIKZG/WM9MARBE
Q+IEYGRW+LL4U+FKZHB9OWAJC9F9+KESKZ89MKHWEWGZ+KHAWDVNENPEIXQERIIY
QQKCZEBJELLEBXWCDORBEMK3WBQZTAPXLGZTBVZRWFYJPEGAD/PDXLHDGKBEMIAD
YHTU/+JDTEGB4MQY+JJHVBCQYMDLCUFLQLNV/LHVNHYW3A++ANMIXZAMRQBANLL+
FMGNQ8VQGOV88SR4G+U9UE+UES/44XY8JXYK3G9FRVNSUU4SEWNSKDVMJLQS4NSE
CKWYK/OV
```

Hint: `ILUVW, FRPPXWH WKH SHUPXWDWLRQ SDVW WKH ARULQJ. WKHQ IRU HDFK GDWD OLQH WUB DOO SRVVLEOH ZKHHOV DQG VWDUWLQJ SRVLWLRQV DQG FKRRVH WKH RQH WKDW PDALPLCHV WKH LQGHA RI FRLQFLGHQFH. BRX PDB KDYH WR GR WZR OLQHV DW RQFH LI WKHUH DUH PRUH WKDQ RQH JRRG FDQGLGDWHV IRU KLJKHVW LRF.`