Unit 179
Attacking Enigma with cribs (Bombe)

The first step in using a crib is to place it against the ciphertext. We saw in Unit 177 that the Enigma never enciphers a letter to itself, and this property can help place a crib. For example, consider this ciphertext and crib:

```
UWLCDYAPLKYAINQIHXJVKMAFAETANCUBPDBASNRREDDFTGRTBXEWSZMQPNLPDGZV
TFEXMPQLTFYGPALMZXBJWRZWRGYTBNFRTWBUJBDKEACCVRYYOREBUWUWGDBDRYRU
WNECGDVBORVFEPIGHF

THECRIBINTOONEOF
```

This is an incorrect placement, because an E matches:

```
UWLCDYAPLKYAINQIHXJVKMAFAETANCUBPDBASNRREDDFTGRTBXEWSZMQPNLPD...
            THECRIBINTOONEOF
```

There may be several placements that satisfy the condition; here is one:

```
UWLCDYAPLKYAINQIHXJVKMAFAETANCUBPDBASNRREDDFTGRTBXEWSZMQPNLPD...
              THECRIBINTOONEOF
```

For a moment, let's think about a three-rotor Enigma with ring settings fixed and without a plugboard. Suppose that we have a ciphertext and know some of the plaintext (a crib placed correctly). There are two or three choices for the reflector (the Germans did not use reflector A in the war), 8·7·6 = 336 ways to place three of eight rotors in the machine, and 26^3 message keys (starting positions of the three rotors), for a total of 5,905,536 possible keys. This is not a big number for those of us living in the modern age. We can try each of them and check to see if the portion of the ciphertext covered by the crib is decrypted correctly, then run the machine backwards to the start of the ciphertext to find the message key. This is computationally less expensive than calculating the index of coincidence or textual fitness of the decryption. We can hasten the process by checking the first letter and only continuing with the decryption if we have a match; for each key, stop decrypting when a discrepancy arises or we have a successful decryption.

Now consider a three-rotor machine with fixed ring settings, but with the plugboard. There are 26! / (6! · 10! · 2^{10}) = 150,738,274,937,250 ways to plug ten cables into the plugboard (choosing 20 of 26 is 25·24· ··· ·7, which gives 26! / 6!; the other factors account for the fact that the order in which we assign the ten cables is irrelevant, and the order of the two letters for each cable is irrelevant). Now the number of keys has grown to 890,190,309,219,827,525,120. Now we have a big number, and we haven't even included ring settings. Enter the *Bombe*, a machine and strategy by Alan Turing. The strategy is to try only the non-steckered keys and to map out pathways through the machine in its various states as it deciphers a text, and then to use them to form loops. Checking loops for consistency

allows cryptanalysts to rule out the vast majority of keys. Bombe's strength comes from the ability to simulate many Enigma machines simultaneously.

The best way to explain the strategy is to look at the details of an example. Consider the ciphertext and crib that we saw above:

```
UWLCDYAPLKYAINQIHXJVKMAFAETANCUBPDBASNRREDDFTGRTBXEWSZMQPNLPDGZV
TFEXMPQLTFYGPALMZXBJWRZWRGYTBNFRTWBUJBDKEACCVRYYOREBUWUWGDBDRYRU
WNECGDVBORVFEPIGHF
```

```
PUTTHECRIBINTOONEOFTHE
```

The machine used to encrypt it has ring settings 1, 1, 1, and the plugboard has all ten cables in use. Suppose that we found the correct placement of the crib earlier. The next thing we do is to show the correspondence from ciphertext letters to plaintext letters, and the state of the machine for each pair. Remember that the Enigma steps before it enciphers a letter, so when we write E_1, we mean the permutation that the machine uses to encrypt the first letter after it has stepped.

$$\begin{array}{c} \texttt{NQIHXJVKMAFAETAN} \\ E_1 \updownarrow \updownarrow \updownarrow \updownarrow \updownarrow \updownarrow \updownarrow \updownarrow \updownarrow \updownarrow \updownarrow \updownarrow \updownarrow \updownarrow \updownarrow \updownarrow E_{16} \\ \texttt{THECRIBINTOONEOF} \end{array}$$

Now, the full machine E is the steckerless machine M between two plugboards S:

$$E = S^{-1} M S$$

We remember that S is its own inverse (M is, too), so we can drop the "−1," but we keep it for a moment. What we have for the first sixteen letters is

$$\begin{gathered} \texttt{N} = E_1(\texttt{T}) = (S^{-1} M_1 S)(\texttt{T}),\ \texttt{T} = E_1(\texttt{N}) = (S^{-1} M_1 S)(\texttt{N}) \\ \texttt{Q} = E_2(\texttt{H}) = (S^{-1} M_2 S)(\texttt{H}),\ \texttt{H} = E_2(\texttt{Q}) = (S^{-1} M_2 S)(\texttt{Q}) \\ \vdots \\ \texttt{N} = E_{16}(\texttt{F}) = (S^{-1} M_{16} S)(\texttt{F}),\ \texttt{F} = E_{19}(\texttt{N}) = (S^{-1} M_{16} S)(\texttt{N}) \end{gathered}$$

Move an S from the right-hand side to the left of each equation (multiply on the left by S on both sides):

$$\begin{gathered} S(\texttt{N}) = M_1(S(\texttt{T})),\ S(\texttt{T}) = M_1(S(\texttt{N})) \\ S(\texttt{Q}) = M_1(S(\texttt{H})),\ S(\texttt{H}) = M_1(S(\texttt{Q})) \\ \vdots \end{gathered}$$

In other words, the stecker-less machine connects not the letters of ciphertext and crib, but their images under the plugboard's substitution:

$$\begin{gathered} S(\texttt{N}) \overset{M_1}{\longleftrightarrow} S(\texttt{T}) \\ S(\texttt{Q}) \overset{M_2}{\longleftrightarrow} S(\texttt{H}) \\ \vdots \end{gathered}$$

These relationships give us sixteen edges in a graph whose vertices are labeled by $S(\mathsf{A})$, $S(\mathsf{B})$, ..., shown in Figure 179.1. Cryptanalysts call this graph the “menu” for this ciphertext/crib pair.

Nicely, the graph has loops, and they intersect. It helps because if we build an operator that goes around that loop, say from $S(\mathsf{T})$ to $S(\mathsf{N})$ to $S(\mathsf{E})$ and back to $S(\mathsf{T})$, then that operator must not alter $S(\mathsf{T})$. The letter at the vertex that is represented by $S(\mathsf{T})$ must be a fixed point of the permutation that the operator enacts:

$$S(\mathsf{T}) = M_{14}\, M_{13}\, M_1\, S(\mathsf{T})$$

There may be more than one fixed point of this permutation. Because there are other loops that begin and end on $S(\mathsf{T})$, those other loops have their own set of fixed points. The correct $S(\mathsf{T})$ must belong to all sets of fixed points, and so we can usually eliminate some. Also notice that $S(\mathsf{A})$ and $S(\mathsf{O})$ form a loop of their own. Therefore we require that $M_{12}\, M_{15}$ and $M_{15}\, M_{12}$ have at least the same two fixed points. The reason that there must be two and that they be the same is that we can start on $S(\mathsf{A})$ and go either clockwise or counterclockwise around the loop, and we can do the same if we start on $S(\mathsf{O})$.

For each configuration of the stecker-less machine and message key, we generate the first sixteen permutations that it has and calculate the composition in the equation above. If the resulting permutation does not have a fixed point, then we can rule out that configuration and message key combination. If it has one fixed point, then we tentatively assign it to be the partner of T on the plugboard. If there are more than one fixed point, then there are more options for $S(\mathsf{T})$. We can do the same for $S(\mathsf{E})$ and $S(\mathsf{N})$ and for $S(\mathsf{N})$ around the other loops. And don’t forget the $S(\mathsf{A})$-$S(\mathsf{A})$ loop. If at any time we find a contradiction, we rule out the key that we have tried. See Table 179.1 for all of the loops in our example. A loop’s operator is its own inverse (showing why is an exercise), and a permutation and its inverse have the same fixed points, so we only need to write down the operators in one sense (clockwise or counterclockwise).

Suppose for our example we try B, I, II, III and message key AAA at the start of the crib. These are the first sixteen permutations of the machine as it steps from to AAB then AAC then AAD etc.

$$\begin{aligned}
M_1 &= \mathsf{BAQMFEXIHSWPDYTLCVJOZRKGNU}\\
M_2 &= \mathsf{DJRALKWPOBFEYQIHNCXZVUGSMT}\\
M_3 &= \mathsf{ZLEJCUITGDMBKONSVXPHFQYRWA}\\
M_4 &= \mathsf{GCBLWTAKQZHDOSMXIUNFRYEPVJ}\\
M_5 &= \mathsf{OSNIRGFMDPVUHCAJWEBXLKQTZY}\\
M_6 &= \mathsf{WYMVNQZJLHOICEKUFTXRPDASBG}\\
M_7 &= \mathsf{CJAFKDZTPBEUORMIWNVHLSQYXG}\\
M_8 &= \mathsf{XIJUYSLVBCZGNMQWOTFRDHPAEK}\\
M_9 &= \mathsf{LFZRWBYTJISAOVMUXDKHPNEQGC}\\
M_{10} &= \mathsf{TKEZCQYNUWBPVHSLFXOAIMJRGD}\\
M_{11} &= \mathsf{KIWFNDUXBSAOTELQPVJMGRCHZY}\\
M_{12} &= \mathsf{SFKUTBPOXYCRNMHGWLAEDZQIJV}\\
M_{13} &= \mathsf{BAQWLKHGRSFEXTPOCIJNVUDMZY}\\
M_{14} &= \mathsf{TEOFBDZXQKJYRSCVIMNAWPUHLG}\\
M_{15} &= \mathsf{MHYPSWRBZXQVAONDKGEUTLFJCI}\\
M_{16} &= \mathsf{CPASNRHGKUIXZEVBYFDWJOTLQM}
\end{aligned}$$

If we look at the *S*(A)-*S*(O) loop and calculate the permutation of its operator we get

$$M_{12}\, M_{15} \;=\; \texttt{NOJGAQLFVIWZSHMUCPTDERBYKX}$$

This permutation has no fixed points, so we cannot find values for *S*(A) and *S*(O). We have to reject this machine setting and try another.

Now we try B, I, II, III and message key AAB at the start of the crib. The first sixteen permutations of the stecker-less machine are

$$\begin{aligned}
M_1 &= \texttt{DJRALKWPOBFEYQIHNCXZVUGSMT}\\
M_2 &= \texttt{ZLEJCUITGDMBKONSVXPHFQYRWA}\\
M_3 &= \texttt{GCBLWTAKQZHDOSMXIUNFRYEPVJ}\\
M_4 &= \texttt{OSNIRGFMDPVUHCAJWEBXLKQTZY}\\
M_5 &= \texttt{WYMVNQZJLHOICEKUFTXRPDASBG}\\
M_6 &= \texttt{CJAFKDZTPBEUORMIWNVHLSQYXG}\\
M_7 &= \texttt{XIJUYSLVBCZGNMQWOTFRDHPAEK}\\
M_8 &= \texttt{LFZRWBYTJISAOVMUXDKHPNEQGC}\\
M_9 &= \texttt{TKEZCQYNUWBPVHSLFXOAIMJRGD}\\
M_{10} &= \texttt{KIWFNDUXBSAOTELQPVJMGRCHZY}\\
M_{11} &= \texttt{SFKUTBPOXYCRNMHGWLAEDZQIJV}\\
M_{12} &= \texttt{BAQWLKHGRSFEXTPOCIJNVUDMZY}\\
M_{13} &= \texttt{TEOFBDZXQKJYRSCVIMNAWPUHLG}\\
M_{14} &= \texttt{MHYPSWRBZXQVAONDKGEUTLFJCI}\\
M_{15} &= \texttt{CPASNRHGKUIXZEVBYFDWJOTLQM}\\
M_{16} &= \texttt{DLFATCJWYGVBNMZRXPUESKHQIO}
\end{aligned}$$

This time, when we look at the *S*(A)-*S*(O) loop we find

$$M_{12}\, M_{15} \;=\; \texttt{QOBJTIGHFVRMYLUAZKWDSPNECX}$$

which has fixed points at G and H. If this is the correct setting of the machine, then *S*(A) = G and *S*(O) = H, or *S*(A) = H and *S*(O) = G. However, if we look at the *S*(E)-*S*(N)-*S*(T) loop, we find

$$M_{13}\, M_1\, M_{14} \;=\; \texttt{LVRXHZOKANSWFQITDUYPGBJEMC}$$

which has no fixed points. So *S*(E) cannot be assigned a value. We must reject this machine setting.

This game continues. But what happens if we find all the fixed points that we need? Let's consider B, I, II, III and message key AAX. The permutations are

$$\begin{aligned}
M_1 &= \texttt{BAFKTCQNVZDRYHSXGLOEWIUPMJ}\\
M_2 &= \texttt{OCBXGUERJIZTPVAMYHWLFNSDQK}\\
M_3 &= \texttt{UEJOBTPZWCNSRKDGVMLFAQIYXH}\\
M_4 &= \texttt{BAQMFEXIHSWPDYTLCVJOZRKGNU}\\
M_5 &= \texttt{DJRALKWPOBFEYQIHNCXZVUGSMT}
\end{aligned}$$

$$
\begin{aligned}
M_6 &= \texttt{ZLEJCUITGDMBKONSVXPHFQYRWA} \\
M_7 &= \texttt{GCBLWTAKQZHDOSMXIUNFRYEPVJ} \\
M_8 &= \texttt{OSNIRGFMDPVUHCAJWEBXLKQTZY} \\
M_9 &= \texttt{WYMVNQZJLHOICEKUFTXRPDASBG} \\
M_{10} &= \texttt{CJAFKDZTPBEUORMIWNVHLSQYXG} \\
M_{11} &= \texttt{XIJUYSLVBCZGNMQWOTFRDHPAEK} \\
M_{12} &= \texttt{LFZRWBYTJISAOVMUXDKHPNEQGC} \\
M_{13} &= \texttt{TKEZCQYNUWBPVHSLFXOAIMJRGD} \\
M_{14} &= \texttt{KIWFNDUXBSAOTELQPVJMGRCHZY} \\
M_{15} &= \texttt{SFKUTBPOXYCRNMHGWLAEDZQIJV} \\
M_{16} &= \texttt{BAQWLKHGRSFEXTPOCIJNVUDMZY}
\end{aligned}
$$

All of the permutations in Table 179.1 have enough fixed points (go ahead and check). But we have a problem: If we calculate the fixed points for $S(\texttt{T})$ (for example), we get inconsistent answers.

$$
\begin{aligned}
M_{14}\, M_{13}\, M_1 &= \texttt{AMPIKNDXTFYHUELVZQJWSGBORC} \\
M_1\, M_{16}\, M_{11}\, M_{12}\, M_{10} &= \texttt{CBNLDHOWUZSKEIFGJQPVYMATXR} \\
M_1\, M_{16}\, M_{11}\, M_{15}\, M_{10} &= \texttt{MRDLOUQJTZVIWNPAXECFHYSGBK}
\end{aligned}
$$

The first has fixed point at A, the second at B, and the third at N. Since we must assign an unique value to $S(\texttt{T})$, we must reject this machine setting as inconsistent.

After trying the 5,905,536 combinations of reflector, rotors, and message key, far fewer remain. The more loops we have in the graph, and especially if they intersect, the fewer candidates remain. For each candidate, we need to try to work out the remaining plugboard settings and see what we get when we decrypt the entire ciphertext. Here, we will only go through the process for the correct settings of the machine, which are B, I, II, III, ABP. Now let's look at the permutations there and see what we can gleam about the plugboard wiring.

$$
\begin{aligned}
M_1 &= \texttt{SKPMUOYLXQBHDTFCJVANERZIGW} \\
M_2 &= \texttt{HJLWMZNARBQCEGXTKIYPVUDOSF} \\
M_3 &= \texttt{IZRUKPXNAWEOTHLFSCQMDYJGVB} \\
M_4 &= \texttt{UYOMVQLRXPNGDKCJFHZWAETIBS} \\
M_5 &= \texttt{NROYTGFWZXVQUACSLBPEMKHJDI} \\
M_6 &= \texttt{TYQKNXRZOUDMLEIVCGWAJPSFBH} \\
M_7 &= \texttt{HNEOCSJAPGMZKBDIXTFRVUYQWL} \\
M_8 &= \texttt{EQFWACINGLRJZHTSBKPOXYDUVM} \\
M_9 &= \texttt{OKIZVPTMCUBRHYAFWLXGJEQSND} \\
M_{10} &= \texttt{RTHXZONCYUQVSGFWKAMBJLPDIE} \\
M_{11} &= \texttt{XPWGHODEQYRSNMFBIKLVZTCAJU} \\
M_{12} &= \texttt{POQWGIEVFNRUZJBACKYXLHDTSM} \\
M_{13} &= \texttt{QPNGXYDSOVMRKCIBALHWZJTEFU} \\
M_{14} &= \texttt{PLTVYKONMQFBIHGAJZUCSDXWER} \\
M_{15} &= \texttt{KODCXJSRQFAUZYBWIHGVLTPENM} \\
M_{16} &= \texttt{OVEXCNJPMGSZIFAHYUKWRBTDQL}
\end{aligned}
$$

The *S*(A)-*S*(O) mini-loop has fixed points at B, L, M, O, U, and Z. But if we go around the larger loops containing *S*(A), one gives fixed points at A and B, and the other has one at B. These three sets has one element in common: B. So *S*(A) = B, and the plugboard has a cable connecting A and B. Next, *S*(E) only participates in one loop, and it has fixed point C, so the plugboard connects E and C. For F, N, O, and T, we find that the only common fixed points show that the plugboard does not alter these letters. So far, we know this much about the machine at the start of the crib:

B, I, II, III, 1, 1, 1, AB, CE, ABP

If we decipher the corresponding segment of the plaintext, we get

TKBRJUURHTOONEOF

In the second position, Q should decrypt to H, but we have K. One way to fix it is to add a cable H-K, but we could do it with two cables, and there are many ways to choose them. So we skip it and move on to the third letter. There, we need I to decrypt to E, but we got B instead. We already have a cables A-B and C-E, so we can fix this with a cable that connects I to whatever M_3 maps to C. That letter is R, so we add a cable I-R. This affects the fourth letter. With the three cables that we know for certain, we have this decryption and see that the fourth letter has become I:

TKEIJUUIHTOONEOF

The fourth letter of the plaintext segment is H. We already have cable C-E and M_4 maps E-V, so we can complete the chain with a plugboard cable H-V. This is the only way to fix the fourth letter, because a chain from the ciphertext letter to the plaintext letter can only have two plugboard cables, and one has already been determined. Having the cable H-V allows us to revisit the second letter. With the four cables that we have already found, the K in the decryption remains unchanged. The plaintext letter is H, there is a cable H-V, M_2 maps V-U. and the ciphertext letter is Q. The only way to complete the chain is to add cable Q-U. For the fifth letter, the chain is R-I-Z-...-X. So we need cable X-Z. For the sixth letter, the chain is I-R-G-...-J, and we must add cable G-J. With the seven cables that we now know, the decryption is

THECRIBIVTOONEOF

We still need to fix the ninth letter. Its chain is N-N-Y-...-M (remember that N is not steckered), so we add the cable M-Y. We have managed to recover eight of the ten plugboard cables.

Running the machine backward to the beginning of the ciphertext tells us that the message key is ABC. What we know so far about the full key is

B, I, II, III, 1, 1, 1, AB, CE, IR, HV, QU, XZ, GJ, MY, ABC

Decrypting the ciphertext with it gives

```
MLYMXDONAYPUTTHECRIBINTOONEOFTHEWPADAWQUASYSINLOSWAPRLRESIQOYTXT
HENWHESVNTBACKFOTHELLEWSERFORTHECNNLDEHTODIGHTITUPSITIXZTLOMKELN
PTHINTSANTINGTHEMX
```

There are only six letters still unaccounted for that can be used for the remaining two plugboard cables: D, K, L, P, S, W, and we can apply the technique from Unit 178 to find the cables. The index of coincidence of the decryption is 1.415. If we try all possibilities for one more cable, we find the largest IoC for D-L at 1.5647. If we add that to the key and search again, the highest IoC is for S-W at 1.6187. Add it to the list, and the full key becomes

> B, I, II, III, 1, 1, 1, AB, CE, IR, HV, QU, XZ, GJ, MY, DL, SW, ABC

The full plaintext is from *Candle and Crib* by Katherine Frances Purdon:

```
MRSMOLONEYPUTTHECRIBINTOONEOFTHESMALLSQUAREWINDOWSANDDREWITOUTXT
HENSHEWENTBACKTOTHEDRESSERFORTHECANDLESTOLIGHTITUPWITHXITLOOKEDN
OTHINGWANTINGTHEMX
```

> Mrs. Moloney put the Crib into one of the small square windows and drew it out. Then she went back to the dresser for the candles to light it up with. It looked nothing wanting them.

vertex	loop operators
S(A)	$M_{12}\,M_{15}$ $M_{10}\,M_1\,M_{16}\,M_{11}\,M_{12}$ $M_{10}\,M_1\,M_{16}\,M_{11}\,M_{15}$
S(E)	$M_{13}\,M_1\,M_{14}$
S(F)	$M_{11}\,M_{12}\,M_{10}\,M_1\,M_{16}$ $M_{11}\,M_{15}\,M_{10}\,M_1\,M_{16}$
S(N)	$M_1\,M_{14}\,M_{13}$ $M_{16}\,M_{11}\,M_{12}\,M_{10}\,M_1$ $M_{16}\,M_{11}\,M_{15}\,M_{10}\,M_1$
S(O)	$M_{12}\,M_{15}$ $M_{12}\,M_{10}\,M_1\,M_{16}\,M_{11}$ $M_{15}\,M_{10}\,M_1\,M_{16}\,M_{11}$
S(T)	$M_{14}\,M_{13}\,M_1$ $M_1\,M_{16}\,M_{11}\,M_{12}\,M_{10}$ $M_1\,M_{16}\,M_{11}\,M_{15}\,M_{10}$

Table 179.1: Loop operators for the graph in the example. See Figure 179.1.

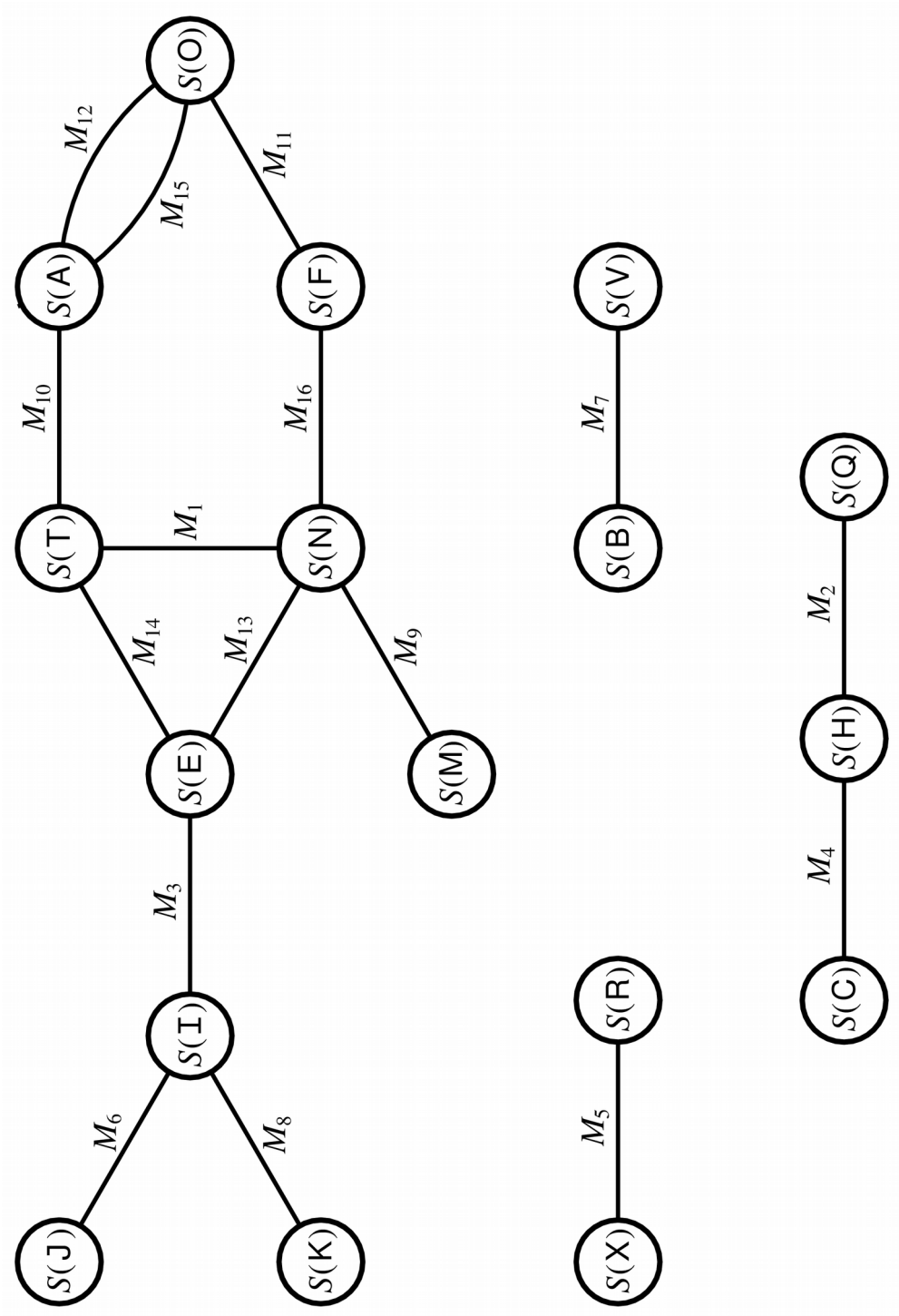

Figure 179.1: Graph (“menu”) for the ciphertext and crib in the example.

Reading and references

Graham Ellsbury, “The Turing Bombe: What it was and how it worked,” 1998, http://www.ellsbury.com/bombe1.htm

Wikipedia, “Bombe,” https://en.wikipedia.org/wiki/Bombe

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

Programming tasks

1. While it is possible to automate the entire process, you may prefer to make the menu and look for loops by hand. If that is the case, then you will create a new program or script for each ciphertext/ crib pair. Finding the solution can take a long time, so we recommend that you use a fast programming language, such as C.

Exercises

1. Explain why the operator/permutation that we get by going around a loop is its own inverse.

2. Here are a ciphertext and crib. The text was encrypted with a three-rotor enigma with ring settings 1, 1, 1. The crib represents the first twenty letters of the plaintext. Decrypt the entire text.

   ```
   TBLIFFTJPMFZPJFTOWMTGKUFQKBBEIQGEHSYFELZOVPCTWPXKCUSJILGAMETZIAG
   JGVATTPPFBHLAQUAQCRLRONUZJUFYWWTFTQTJTQSXMAKFRBOGEXFQHJCOBFIDHAW
   QKODRHPGBUFEJBTETJZYGVAFPKZFKGJ

   IAMABOUTTOGIVEYOUTHE
   ```

   If you enjoyed this exercise, there is a similar challenge at MysteryTwister: https://mysterytwister.org/media/challenges/pdf/mtc3-hoerenberg-02-turing-en.pdf