1 Cryptography: An Overview

1.2 Enigma

Problem 4. *Consider the notion of "evolution" that we introduced in this section. We can formulate this notion mathematically as follows. For a given initial setting of the machine, as determined, for example, by the daily key, let P_m be the permutation executed by the machine after m keystrokes. We considered a case in which, for some unknown letter x, $P_0 x = Q$ and $P_3 x = E$. This is what we meant by saying that Q "evolves" into E. Evidently the permutation that expresses this evolution is $P_3 P_0^{-1}$. (Applying P_0^{-1} to Q gives x, and then applying P_3 gives E.) Show that the cycle lengths of the "evolution" $P_3 P_0^{-1}$ are indeed independent of the plugboard permutation A, as was noted by Rejewski. (Note that the permutation P_m is given by Eq. (1.3) with appropriate values of n_1, n_2, and n_3.)*

Intuitively, the cycle lengths won't be affected by any setting of the plugboard as the plugboard statically shuffles the characters the rotor-reflector assembly receives and provides. The problem can be rigorously outlined as it was by Rejewski using the following equation, where A represents the involution of the plugboard ($A = A^{-1}$), S^n represents the effect of rotating n times, R_i represents the i-th rotor, and B represents the reflector.

$$A^{-1}(S^{-n}R_1S^n)^{-1}B(S^{-n}R_1S^n)A$$

The equation above represents the permutations a one-rotor Enigma machine would act on input, where n is incremented once per letter modulo 26. In group theory[1] the closed operation $A^{-1}(\dots)A$ represents a *congugacy* where the plugboard's involution doesn't affect the cycle length of the permutation it conjugates, i.e. $P^m = A^{-1}R^mA$. Therefore Rejewski concludes that the cycle lengths are consistent across all plugboard configurations, significantly reducing the number of combinations. After documenting the cycles, one can simply treat this iteration of the Enigma machine as a substitution cipher, to my knowledge.

Remark. I'd be curious to know how other students are rigorously outlining this answer; I may be reading into this question too much or I missed the lecture on congugacy. I remember this idea being briefly outlined in the introductory Linear Algebra course via matrix similarity, but I don't know if the average student would make the connection or be able to say much more than "because that's how it is with matrices" which is really just a case within non-abelian groups. The intuitive answer is too obvious and the rigorous answer too rigorous for this text, in my humble opinion. Ignore this if it was explained explicitly in class.

Problem 5. *Consider the Enigma machine with a certain initial setting of the rotors and plugboard. With this initial setting, let P_0 be the permutation the machine applies to the first letter of the plaintext, and let P_3 be the permutation that it applies to the fourth letter of the plaintext. Recall the following two facts about the permutations P_0 and P_3:*

(i) $P_0^{-1} = P_0$ *and* $P_3^{-1} = P_3$*;*

[1] I think this is right; I haven't formally studied group theory and am working off of my first impressions from Wikipedia.

(ii) P_0 does not send any letter to itself, and neither does P_3.

These facts will be useful in this problem.

We have seen how cryptanalysts were able to crack Enigma by considering the lengths of the cycles of the permutation $P_3P_0^{-1}$. Let $y_1, y_2, \ldots, y_m$ be a cycle of this permutation. That is, the y_i's are m distinct letters of the alphabet, and $P_3P_0^{-1}y_1 = y_2, P_3P_0^{-1}y_2 = y_3, \ldots, P_3P_0^{-1}y_m = y_1$.

1. *Show that $P_0y_m, P_0y_{m-1}, \ldots, P_0y_1$ is also a cycle of $P_3P_0^{-1}$.*
2. *Show that the cycle defined in part (a) consists entirely of letters that do not appear in the original cycle $y_1, y_2, \ldots, y_m$. It follows that the cycle lengths always come in matching pairs.*

Tackling the first subproblem, we will show that applying the permutation $P_3P_0^{-1}$ to a letter y_i sends it backwards (i.e. lowers the index) in the cycle to y_{i-1} given i modulo m. Suppose we have a permutation acting on a cycle element such that $P_3P_0^{-1}(P_0y_i)$. We can say that, using the $y_i = P_3P_0^{-1}y_{i-1}$ definition from the problem statement and knowing P_0 and P_3 are involutions, that

$$\begin{aligned} P_3P_0^{-1}(P_0y_i) &= P_3P_0^{-1}(P_0P_3P_0^{-1}y_{i-1}) \\ &= P_3(P_0^{-1}P_0)P_3P_0^{-1}y_{i-1} \\ &= (P_3P_3)P_0^{-1}y_{i-1} \\ &= P_0^{-1}y_{i-1} = P_0y_{i-1} \end{aligned}$$

and thus $P_3P_0^{-1}$ sends P_0y_i to P_0y_{i-1} in a cyclic fashion $i \pmod{m}$.

For the second subproblem, lets assume that there is overlap between the plaintext and the ciphertext sets such that $y_i = P_0y_j$. This implies that $y_j = P_0y_i$ (as P_0 is an involution) and thus the two letters are paired. However this would suggest that P_0 can send a letter to another letter between sets and that one doesn't need $P_3P_0^{-1}$ to create the second set, which is established as false by the problem statement. Thus the sets must be disjoint and the letters are paired.

1.3 A Review of Modular Arithmetic and $\mathbb{Z}_n$

Problem 1. *Write out the addition and multiplication tables for $\mathbb{Z}_3$, $\mathbb{Z}_4$, and $\mathbb{Z}_7$.*

First, the addition tables ($\mathbb{Z}_n^+$).

$\mathbb{Z}_3^+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\mathbb{Z}_4^+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\mathbb{Z}_7^+$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Next, the multiplication tables ($\mathbb{Z}_n^\times$).

$\mathbb{Z}_3^\times$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbb{Z}_4^\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\mathbb{Z}_7^\times$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Problem 4. *Show that addition and multiplication modulo n are well defined. In other words, show that if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$.*

In order to show that the addition and multiplication operations endowed to the $\mathbb{Z}_n$ ring are well defined, we need to show that both $(\mathbb{Z}, +)$ and $(\mathbb{Z}_n, \cdot)$ used in a mapping won't produce two different, valid results in the range, i.e., for $f : a \mapsto b$ we need a unique value $b \in \mathbb{Z}_n$ given $a \in \mathbb{Z}_n$.

To start, we can rewrite the statements $a \equiv b \pmod{n}$ as $a = b + in$ and $c \equiv d \pmod{n}$ as $c = d + jn$ for some $i, j, n \in \mathbb{Z}$. For the addition operation, we can say that

$$\begin{aligned} a + c = (b + in) + (d + jn) &\implies a + c = b + d + n(i + j) \\ &\implies a + c = b + d \pmod{n}, \end{aligned}$$

a unique element in $\mathbb{Z}_n$. For the multiplication operation, we can say

$$\begin{aligned} a \cdot c = (b + in) \cdot (d + jn) &\implies bd + b(jn) + d(in) + (in)(jn) \\ &\implies a \cdot c = b \cdot d + n(bj + di + ijn) \\ &\implies a \cdot c = b \cdot d \pmod{n} \end{aligned}$$

which is a unique element in $\mathbb{Z}_n$. Thus, both addition and multiplication are well defined binary operations in $\mathbb{Z}_n$ meaning their results do not depend on the choice of representatives in each equivalence class.

Matrix Practice

We are given $M = \begin{pmatrix} 2 & 3 & 9 \\ 3 & -1 & 2 \\ 4 & -4 & 7 \end{pmatrix}$. Below, each product is computed and explained.

Problem 1. $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} M$

We have

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} M = \begin{pmatrix} 3 & -1 & 2 \\ 2 & 3 & 9 \\ 4 & -4 & 7 \end{pmatrix}.$$

Multiplying on the left by this permutation matrix swaps the first two rows of M.

Problem 2. $M \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

Right multiplication by this matrix swaps the first and second columns of M. In particular, since the first column of the product becomes the second column of M and vice versa, we obtain

$$M \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 2 & 9 \\ -1 & 3 & 2 \\ -4 & 4 & 7 \end{pmatrix}.$$

Problem 3. $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} M$

This left multiplication rearranges the rows of M: the first row becomes the third row of M, the second row remains unchanged, and the third row becomes the first row. Thus,

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} M = \begin{pmatrix} 4 & -4 & 7 \\ 3 & -1 & 2 \\ 2 & 3 & 9 \end{pmatrix}.$$

Problem 4. $M \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$

Right multiplication by this matrix permutes the columns of M: the first column of the product comes from the third column of M, the second from the second column, and the third from the first column. Therefore,

$$M \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 9 & 3 & 2 \\ 2 & -1 & 3 \\ 7 & -4 & 4 \end{pmatrix}.$$

Problem 5. $\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} M$

Left multiplication by a diagonal matrix multiplies each row by the corresponding diagonal entry. Here, the first row is multiplied by 2 while the other rows remain unchanged:

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} M = \begin{pmatrix} 4 & 6 & 18 \\ 3 & -1 & 2 \\ 4 & -4 & 7 \end{pmatrix}.$$

Problem 6. $M\begin{pmatrix}2 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}$

Right multiplication by this diagonal matrix multiplies each column by the corresponding diagonal entry. Thus, the first column of M is multiplied by 2, yielding

$$M\begin{pmatrix}2 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix} = \begin{pmatrix}4 & 3 & 9\\ 6 & -1 & 2\\ 8 & -4 & 7\end{pmatrix}.$$

Problem 7. $\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 3\end{pmatrix}M$

Here, only the third row of M is multiplied by 3:

$$\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 3\end{pmatrix}M = \begin{pmatrix}2 & 3 & 9\\ 3 & -1 & 2\\ 12 & -12 & 21\end{pmatrix}.$$

Problem 8. $M\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 3\end{pmatrix}$

Right multiplication by this matrix multiplies the third column of M by 3:

$$M\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 3\end{pmatrix} = \begin{pmatrix}2 & 3 & 27\\ 3 & -1 & 6\\ 4 & -4 & 21\end{pmatrix}.$$

Problem 9. $\begin{pmatrix}1 & 1 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}M$

Left multiplication by this matrix adds the second row of M to its first row. Explicitly, the new first row becomes

$$(1)(\text{row } 1) + (1)(\text{row } 2) = (2+3,\ 3+(-1),\ 9+2) = (5, 2, 11).$$

Thus,

$$\begin{pmatrix}1 & 1 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}M = \begin{pmatrix}5 & 2 & 11\\ 3 & -1 & 2\\ 4 & -4 & 7\end{pmatrix}.$$

Problem 10. $M\begin{pmatrix}1 & 1 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}$

Right multiplication by this matrix adds the first column of M to its second column. In other words, the new second column is

$$\text{(column 1)} + \text{(column 2)} = \begin{pmatrix} 2+3 \\ 3+(-1) \\ 4+(-4) \end{pmatrix} = \begin{pmatrix} 5 \\ 2 \\ 0 \end{pmatrix}.$$

Thus,

$$M \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 5 & 9 \\ 3 & 2 & 2 \\ 4 & 0 & 7 \end{pmatrix}.$$

Problem 11. $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} M$

The left multiplication by this permutation matrix cycles the rows: the first row becomes the second row of M, the second row becomes the third row, and the third row becomes the first row. Hence,

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} M = \begin{pmatrix} 3 & -1 & 2 \\ 4 & -4 & 7 \\ 2 & 3 & 9 \end{pmatrix}.$$

Problem 12. $M \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$

Right multiplication by this matrix permutes the columns of M. The new first column is the original third column, the new second is the original first, and the new third is the original second. Thus,

$$M \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 9 & 2 & 3 \\ 2 & 3 & -1 \\ 7 & 4 & -4 \end{pmatrix}.$$

Problem 13. $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} M$

Here, the left multiplication rearranges the rows so that the first row of the product is the third row of M, the second row is the first row of M, and the third row is the second row. That is,

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} M = \begin{pmatrix} 4 & -4 & 7 \\ 2 & 3 & 9 \\ 3 & -1 & 2 \end{pmatrix}.$$

Problem 14. $M \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$

Right multiplication by this matrix permutes the columns of M: the new first column is the original second column, the new second is the original third, and the new third is the original first. Thus,

$$M\begin{pmatrix}0 & 0 & 1\\ 1 & 0 & 0\\ 0 & 1 & 0\end{pmatrix} = \begin{pmatrix}3 & 9 & 2\\ -1 & 2 & 3\\ -4 & 7 & 4\end{pmatrix}.$$

Problem 15. $\begin{pmatrix}0 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 0\end{pmatrix} M \begin{pmatrix}0 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0 & 1\end{pmatrix}$

The left matrix selects only the second row of M and zeros out the others. The right matrix selects only the third column. Since the $(2, 3)$ entry of M is 2, we obtain

$$\begin{pmatrix}0 & 0 & 0\\ 0 & 0 & 2\\ 0 & 0 & 0\end{pmatrix}.$$

Problem 16. $\begin{pmatrix}0 & 0 & 1\\ 0 & 0 & 0\\ 0 & 0 & 0\end{pmatrix} M \begin{pmatrix}0 & 0 & 1\\ 0 & 0 & 0\\ 0 & 0 & 0\end{pmatrix}$

The left matrix picks out the third row of M and places it in the first row, while the right matrix selects only the first column of the result. Since the $(3, 1)$ entry of M is 4, the final product is

$$\begin{pmatrix}0 & 0 & 4\\ 0 & 0 & 0\\ 0 & 0 & 0\end{pmatrix}.$$