Tony Majestro

Problem Set 4

1. With this set of six-letter starts, you have enough data to determine the cycle decompositions of and , where and the first six ENIGMA permutations for that day. For this exercise, your job is to find those cycle decompositions.



The output for the above program gives the following cycle decompositions:

* (ATWRNZKOPS) (BVLQDMFEUJ) (CX) (G) (HI) (Y)
* (ASHRLWBKU) (COFXTNPVY) (DZG) (EIM) (J) (Q)
* (AFXKNRDCVYSUJ) (BOQZPMLIWTEGH)

1. As we mentioned in class, in those days the transmission channels were very noisy, and sometimes there were mistakes in sending the six-letter string. The above list of six-letter starts contains one string that has an incorrect letter. Find that string, and identify the error.

To figure out which message contains the error, we can begin by generating the mappings that represent the cycle decompositions for each set of permutations just as in problem 1. We can then compare the values in each message to the values in each map. If we find a value that does not equal the value in cycle map, then we have found the incorrect letter and thus the incorrect message.

We can assume that the mappings generated in problem 1 are correct. This is because the code for printing the cycles in problem 1 would have raised an exception if it encountered a key to end the cycle whose value was not the first value in the cycle. The following code finds the message with the incorrect letter mapping:





The output for the above program gives the following error and correction:

Incorrect letter: C

Incorrect message: YEFYIC

Corrected letter: X

Corrected message: YEFYIX

1. 3. Suppose and . Write as a product of disjoint cycles.

To begin, we can start with 1 and figure out the product of disjoin cycles by figuring out what 1 maps to in and use that value to figure out what it maps to in . This gives 1 maps to 2 in and 2 maps to 5 in . Therefore, in , we have that 1 maps to 5.

This process can be repeated:

* 1 maps to 2 in , 2 maps to 5 in
* 5 maps to 1 in , 1 maps to 7 in
* 7 maps to nothing in , 7 maps to 4 in
* 4 maps to 5 in , 5 maps to 8 in
* 8 maps to nothing in , 8 maps to 9 in
* 9 maps to nothing in , 9 maps to 2 in
* 2 maps to 3 in , 3 maps to 6 in
* 6 maps to nothing in , 6 maps to 3 in
* 3 maps to 4 in , 4 maps to 1 in

This gives the following product:

1. One of the design “features” of the ENIGMA machine is that no letter maps to itself – that is, it has no fixed points. Another word for such a permutation is a derangement. Find the number of derangements for n = 1, 2, 3, 4 and 5.

We can find the number of derangements for a given n by calculating all of the permutations for a set of size n, and count the number of such permutations that are derangements. The following program calculates the number of derangements for a given set of size 1, 2, 3, 4, and 5:



This program gives the following output:

Num derangements for n = 1: 0

Num derangements for n = 2: 1

Num derangements for n = 3: 2

Num derangements for n = 4: 9

Num derangements for n = 5: 44