Fieldwork Assignment

Stuart Boersma, 2021
Stuart.boersma@cwu.edu

Overview:

For the rest of this quarter, you will play the daily role of the Polish Codebreakers which followed a schedule like:

1. Intercept enough messages so one can use the first six letters to determine the three products: DA, EB, and FC.
2. Determine the cycle structure of these three permutations and look them up in your directory. If you're lucky, this will give you the rotor order, ring settings, and initial rotor positions (the ground setting) that every Enigma operator will use for that day. If you're unlucky… you may have several settings to try and you should plan for a long day at work. Note: this will essentially give you all you need to know about the daily key **except for the plugboard settings**.
3. Using the "Psychology" method or given a little extra information about operator habits, you might get lucky and be able to come up with a unique way to factor DA, EB, and FC into the six permutations: A, B, C, D, E, F.
4. Knowing A, B, C, D, E, F, you can now decrypt all of the first six characters of any message. That is, you can determine the message key that each operator chose at random.
5. If you are in possession of a "crib" (a known piece of plaintext) or can guess a "crib", you can use that to help you determine plugboard settings.
6. Once you are in possession of the plugboard settings, you now have the complete Daily Key and should be able to read any message sent that day.

Assumptions:

1. We are not really dealing with ring settings, we will assume they are set at A, A, A.
2. Messages are encrypted with the indicator method:
    1. Set up Enigma according to Daily Key
    2. Pick three random letters for the message key. Encrypt them twice. Write down these six letters.
    3. Turn rotors to your message key and encrypt the message.
    4. Send the first six letters together with the encrypted message.
3. Word breaks are not kept when using Enigma, but the ciphertext is often written in groups of five characters to make it easier to read. In this assignment, I've also made the first six letters more obvious by writing them in two groups of three.
4. All messages are in English.

Fieldwork I

Download and print the Intelligence Report above and use the session key intercepts to determine the three product permutations: DA, EB, FC.

1. Write DA as a product of disjoint cycles.

2. Write EB as a product of disjoint cycles.

3. Write FC as a product of disjoint cycles.

The cycle structures of these three permutations can help determine the Daily Key for the Enigma. Submit your assignment and I will respond in the assignment comments with information regarding the Daily Key.

[this is the end of the assignment, but I wanted to emphasize the mathematics that is involved in the above work]

The Mathematics Used in this step:

- A little clever thinking.
- The fact that every permutation can be written as the product of disjoint cycles.
- The fact that the cycle structure of conjugate permutations is the same means we can recover most of the daily key without worrying about the huge number of possible plugboard combinations.

Fieldwork II

Factor your permutations DA, EB, FC to determine the six permutation A, B, C, D, E, F. Recall that these should all be legitimate Enigma permutations. That is, they should swap 13 pairs of letters.

1. What are the six permutation A, B, C, D, E, F?

2. What message key did Operator 1 pick?

3. What message key did Operator 2 pick?

4. Do these seem like random message keys?

Note: Completing this Fieldwork assignment with the given information will earn you extra bragging rights. If you want an easier time of it.... ask me for a hint and I can tell you which operators typed the message keys WWW, AAA, and QQQ.

[this is the end of the assignment, but I wanted to emphasize the mathematics that is involved in the above work]

The Mathematics Used in this step:

- Factoring these permutations uses what I call the "Finger Theorem", but this is actually a fairly important theorem in the theory of permutations.
- While not mathematics, per se, we are also using the fact that humans are humans and are very bad at picking randomly and very good at being lazy.
- Clever thinking and puzzle solving comes in handy as well.

Fieldwork III

You should know the message key that Operator 1 used to encrypt his weather report. If you set up your Enigma according to what you know about the Daily Key, you can then turn the rotors to match the message key. Using the "crib" about how the message begins, you can encrypt this plaintext crib and compare the resulting ciphertext to what Operator 1 actually sent. It probably does not match exactly because you do not know the plugboard setting for the Daily Key. Try adding a single plugboard setting, re-encrypting, and compare. If things are better, that's good. If not, maybe that wasn't the right plugboard setting. Keep adjusting the plugboard settings until you can encrypt the crib and have it match exactly what Operator 1 sent. Most Daily Keys used 0-6 plugboard settings.

1. What are the plugboard settings? You can report your settings by listing the pairs of letters that are connected. For example if A and B are connected, report: AB.

2. What is the complete message that Operator 1 sent?

[this is the end of the assignment, but I wanted to emphasize the mathematics that is involved in the above work]

The Mathematics Used in this step:

- While we know where the crib goes in this assignment, in other situations you may need to try "crib dragging". The "crib dragging" method uses the fact that Enigma never encrypts a letter to itself. This is a result of the fact the every Enigma permutation is conjugate to the reflector, so it must swap 13 pairs of letters.
- General problem solving and perseverance are important here and elsewhere in mathematics!

Fieldwork IV

Decrypt the message from Operator 13 and save the day.

1. What is the message from Operator 13?