

BUILDING A BOMBE

The Mathematics and Circuitry that Bested German Encryption

Jonah Weinbaum

Contents

| | | |
|----------|------------------------------|----------|
| 1 | The UK Bombe | 1 |
| 1.1 | Motivating Example | 1 |
| 1.2 | Changes to Enigma | 1 |
| 1.3 | Loops | 3 |
| 1.4 | Test Function | 3 |

Chapter 1

The UK Bombe

Section 1.1

Motivating Example

Section 1.2

Changes to Enigma

Starting in 1940, the German's enhanced the security of their key distribution. As discussed in CITE the *Grundstellung* rotor position was sent along with the daily key and an operator chose a *Spruchschlusse* to encode twice at the start of a message. Later iterations of this protocol removed the *Grundstellung* from key sheets.

These new key sheets contained the following columns columns *Tag/Datum*, *Walzenlage*, *Ringstellung*, *Steckerverbindungen*, and *Kennggruppen*

Notice the removal of the *Grundstellung* as well as the addition of the *Kennggruppen*. The *Kennggruppen* were a set of four trigrams used to identify which setting was being used to encode a message, this is particularly useful if trying to decode a message using

a prior day's key. The operator would choose a trigram from the the *Kenngruppen*, append two letters to the front of the trigram, and this five letter combination (known as the *Buchstabenkenngruppe*) would precede the message being sent. If a message was sent in multiple segments, multiple *Buchstabenkenngruppe* were used to start each segment.

When sending a message the operator was to use the following protocol

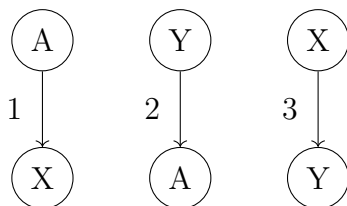
- I. The time at which the message was sent is listed
- II. The number of parts which the message contained is listed
- III. Which message part is being sent is listed
- IV. The length of the message part (not including *Buchstabenkenngruppe*) is listed
- V. A *Grundstellung* rotor position is chosen and listed
- VI. A *Spruchschlüssel* rotor position is chosen and encoded using the *Grundstellung*, this is listed
- VII. The *Buchstabenkenngruppe* is listed
- VIII. The message part encoded using the daily key and the *Spruchschlüssel* position is listed

It is clear that with this protocol, the Polish Bomba could no longer deduce the necessary details to decrypt enigma messages. All of the permutation information contained in the original key distribution protocol was removed and a new method needed to be derived for inferring information about the daily key.

Section 1.3

Loops

The removal of the double encoded *Spruchschlüssel* does not mean that permutation information cannot be stored elsewhere in the message. For the sake of argument, let us say we knew that our message had plaintext encoding



Where the number in each mapping indicates how many steps away we are from the rotor positions when we began encoding the message.

Section 1.4

Test Function

We begin by defining a new notion of permutation order that will ease notation going forward.

Definition 1.1. For $\sigma \in S_n$ and $k \in \mathbb{N}_n$, the **permutation order with respect to k** is the smallest integer $i \in \mathbb{N}$ such that

$$\sigma^i(k) = k$$

We denote that as $\text{ord}_k(\sigma)$.

This is distinct from $\text{ord}(\sigma)$ since this does not require that $\sigma^{\text{ord}(\sigma)}$ is the identity on all elements, rather we just require this on a single element k .

We define a test function which we will use to test our hypotheses of steckerings in the plugboard.

Definition 1.2. The **Enigma test function** on n letters is

$$\begin{aligned} \tau : S_n \times \mathbb{N}_n &\rightarrow \mathbb{N}_{2^n} \\ (\sigma, k) &\mapsto \sum_{i=1}^n b_i \cdot 2^{i-1} \end{aligned}$$

Where

$$b_i := \begin{cases} 1 & i \in \bigcup_{i=1}^{\text{ord}_k(\sigma)} \{\sigma^i(k)\} \\ 0 & \text{else} \end{cases}$$

Let us break down this function since there appears to be a lot of verbose notation. To step back for a moment, our goal with this test function is to examine how current will flow through a loop when applied to a possible steckering.

We first consider the case where both our rotor stack σ and hypotheses k are correct. Then the loop immediately closes and we have that for our test

$$\sigma(k) = k$$

In this case $\text{ord}_k(\sigma) = 1$. We then have that $\bigcup_{i=1}^{\text{ord}_k(\sigma)} \{\sigma^i(k)\}$ reduces to $\{\sigma(k)\} = \{k\}$. Then it is clear that only b_k will be non-zero and thus

$$\tau(\sigma, k) = 2^k$$

This represents an n -bit number with also zeros aside from the k -th position. This is analogous to only the k -th wire being live in our Bombe.