BUILDING A BOMBE

The Mathematics and Circuitry that Bested German Cryptographers

Jonah Weinbaum

Contents

1 The Enigma **1**

2 Permutations **2**

3 The Polish Bomba **3**

4 The UK Bombe **4**

4.1 Motivating Example 4

4.2 Changes to Enigma 4

4.3 Loops 6

Chapter 1

The Enigma

Chapter 2

Permutations

Chapter 3

The Polish Bomba

Chapter 4

The UK Bombe

Section 4.1

Motivating Example

Section 4.2

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 *Kenngruppen*

Notice the removal of the *Grundstellung* as well as the addition of the *Kenngruppen*. The *Kenngruppen* 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 preceed 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

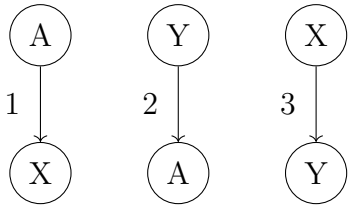
VIII. The message part encoded using the daily key and the *Spruchschlüssel* position is listed

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 infering information about the daily key.

Section 4.3

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.