JYI Journal of Young Investigators RESEARCH ARTICLE

An Examination of the Components and Mathematics of the Enigma Electromechanical Rotor Ciphers

Kristi Short[1] and Aharon Dagan[2]

This paper describes the mathematics of the Enigma electromechanical rotor ciphers used by Germany during WWII. The research is focused on the contributions made by the Polish Cipher Bureau and presents their incentives for breaking Enigma encryptions. German operational procedure is included to show how redundancy measures allowed frequency analysis to be enabled, easing Polish efforts. Also included are the calculations for the strength of encryption granted by each component. Research focuses on the three-rotor configuration of the Wehrmacht Enigma variant used by the German Army in 1932. Also presented are examinations of the mathematical solutions of Marian Rejewski in order to show the method of decoding as well as the significance of contributions from the Polish Cipher Bureau prior to the beginning of World War II. This paper shows why it is important to calculate the practical as well as theoretical encryption strength of a cipher method. Also, that it is important to eliminate redundancy methods whenever possible.

INTRODUCTION

The focus of this paper is the Polish contribution to breaking Axis power encryptions during World War II (WWII). The Polish had more incentive due to the geographical positioning than any other country and could not accept that the Enigma was flawless. For this reason, research is limited to the Wehrmacht Enigma machine used by the German Army starting from 1932 and broken by the Polish. The invention of electromechanical cipher devices such as the Enigma machines allowed for the creation of increasingly complex algorithms that would have never been feasible with the pen and paper methods of classical cryptography. This report shows why the German World War II military relyed on the Enigma cipher, as well as why this confidence was undeserved.

Included are details of the physical components of the Enigma cryptosystem as well as the security imparted by each component. An aalysis of Rejewski's permutation notation of the ciphers with respect to their components is also included. This paper attempts to place the Enigma cipher mathematics in their proper historical context in a brief, easy to understand format.

History

Polish involvement in World War Two

The German engineer Arthur Scherbius invented the Enigma electromechanical rotor cipher towards the end of World War I (WWI) for the banking industry. However, due to reparations Germany was experiencing a period of hyperinflation, and the device did not sell.Scherbius marketed the Enigma to the German Navy next, but due to the country's economic situation at the end of WWI, they initially did not purchaseit and the machines were offered commercially (Mowry 2003.

Only five years after WWI Winston Churchill released "The World Crisis", in which he disclosed that the Allies had routinely read German Naval messages sent during the war.This announcement took the Germans entirely by surprise, and generated a rumor that Germany had not actually lost the war.The 'stab-in-the-back'legend stated that Germany had not lost but had been betrayed by republicans and civilians who had overthrown the monarchy (Tucker and Roberts 2005).Shortly after Churchill's remarks, Rudolph Thilo-Schmidt, Chief of Staff of the German Signal Corps, purchased over 30,000 Enigma machines from ChiffriermaschinenAktien-Gesellschaft (Cipher Machines Stock Corporation chaired by Scherbius and E. Richard Ritter). Almost immediately, the English and French could no longer decrypt German communications. Germany's main encryption method was now Enigma (Perry 2010).
Ironically, Rudolph Thilo-Schmidt's brother, Hans Thilo-Schmidt, sold codebooks to the French(Wilcox 2006).The French made no progress even with the codebooks, and they passed them to the Polish(as per the Franco-Polish Warrant Agreement, 1925).

The first break in the Enigma cipher came from The BiuroSzyfrow (Polish Cipher Bureau) in Warsaw. In 1932, three recent mathematics graduates from PoznańUniversity-- Marian Rejewski, Jerzy Rozycki and HenrykZygalski-- were recruited to the Polish Cipher Bureau (Kull 2007). These three mathematicians, known as the 'Great War Time Polish Geniuses', first broke Enigma's ciphers in December, 1932. The break was facilitated by the codebooks passed by the French to the Polish. Rejewski had already determined cornerstoneequations for the wiring of the rotors but still had variables to understand. The key settings indicated in the codebooks provided enough information to fill in Rejewski's unknowns and complete his system of equations modeling the functions of the Enigma. The subsequent development of Rejewski's "Enigma Doubles" soon followed (Christensen 2007).

[1]Mills College, 5000 MacArthur Blvd.,Oakland, CA 94613 [2]Santa Fe College, 3000 NW 83rd St., Gainesville, FL, 32606

*To whom correspondence should be addressed: witchtacular@gmail.com

In July 1939, Polish, French and British Intelligence Services met for a conference at Pyry near Warsaw. Here the Polishrevealed they had broken Enigma and promised an Enigma Double to both countries. The Polish delivered their equipment and techniques for breaking Enigma to British and French intelligence. The Polish breakthrough helped the Allies develop one of the most important weapons of World War II, Alan Turing's cryptographic bomba.Turing's electromechanical device, which the Allies codenamed "Ultra", was able to solve the daily settings of the German Enigma machines.

Additionally, Turing's bomba decrypted the specialized Lorenz 40 and 42 ciphers used by German high command, Italian ciphers such as Hagelin, and Japan's JN-25 and Purple ciphers. Winston Churchill would tell King George the VI after World War II ended, "It was thanks to Ultra that we won the war."

German Operational Procedures

Under the correct set of procedures, the military variants of Enigma would have been unbreakable. However, the Germans never used the machine to the maximum capacity.

The largest exploitable weakness did not actually come from the machine itself but was due to the German operating procedure. The problem came in the transmission of these ciphered messages. In order for Enigma communications to be read, both sending and receiving machines had to have matching settings. At the time of the Rejewski decryptions, and until September 15, 1938 (Rejewski1980, German set-up of the Enigma had the following specifications:

1. The three rotors were set up in the machine in an order specified by the codebooks provided by German intelligence.
2. After the rotor assembly was placed in the machine, the plugboard sockets were paired and connected. The plugboard settings were also designated by the codebooks.
3. The letter ring on each rotor was adjusted to show a sequence of three letters in the window on top of the machine chosen by the operator.
4. Finally, the three letters were then enciphered by the machine, twice. This meant that the first six letters (or preamble) were really just a pair of three letters ciphered, each with different alphabets twice. The analyst would know that the first letter eventually changed into the fourth letter, the second letter changed into the fifth letter, and the third letter changed into the sixth letter.

The setup procedure, particularly the redundancy measure of ciphering the letters twice, allowed Rejewski to deduce the wiring of the rotors and eventually the entire Enigma machine.

Components

Before we discuss the Enigma encryptions, we must first talk about the components of the Enigma machines.

The Keyboard

German: Tastatur

The Enigma machines used a bi-directional keyboard with 26 keys. Bi-directional keyboards are capable of both sending and receiving commands from the system. Modern keyboards are all bi-directional in design and function.

Standard North American keyboards have a QWERTY setup for the position of letters on the keys; counterparts in Eastern Europe have a QWERTZU setup similar to the setup of the German Enigma machines later in the war. At the time of the Polish break, the keyboard setup was unknown; Rejewski deduced that the Enigma keyboard was laid out alphabetically (Copeland 2004).

When a key is pressed on the keyboard, an electrical circuit is completed. The current then passes from the keyboard through each of the components ultimately lighting up a bulb on the light-board indicating the new ciphertext letter. In addition, when a letter is pressed on the keyboard, before any enciphering of the messages takes place the right-most rotor advances forward one-step. In other words, when a key is pressed, a current is released into the machine causing the components to begin the ciphering process.

The Lightboard

The lightboard has the same 26 characters as the keyboard and is arranged in the same order. When a key is pressed, the current runs through each of the components and the corresponding ciphertext letter lights up on the lightboard. The new ciphertext letter was then either recorded by the operator, or transmitted through radio channels (Rejewski 1982).

The Plugboard

German: Steckerbrett

The plugboard is the first variable component of the Enigma. The plugboard is located on the front of the machine and contains 26 sockets, one for each letter in the alphabet. The Plugboard generates a great deal of Enigma's cryptographic strength (its large key space). In order to read messages sent by Enigma the receiver must have the same plugboard setup. The daily setup of the plugboard was determined by codebooks distributed to operators from German intelligence.

A rangefrom zero to thirteen dual-wired cables (Steckerverbindungen) can be plugged into the plugboard allowing pairs of letters to be transposed. When electriccurrent reaches the plugboard, it changes its path if the letter is socketed to another letter. For instance, suppose the letter 'B' is left un-socketed then 'B' is wired directly to the 'B' input on the rotors.

At the time of the Polish attack (1932), the Germans were using a standard set of six plugboard cables (Christensen 250). In 1941, they standardized the use of ten cables (Miller 17)., that gives 150,738,274,937,250 possible plugboard connections. The effect of using ten cables in the plugboard is the pairing of twenty letters with the remaining six passing through the plugboard unchanged. After the standardization of ten cables, no additional cables were added even though the addition of one

more cable would have given the maximum number of possible plugboard connections.

The Rotor Assembly

German: Chiffrierwalzen

The rotor assembly contains three of Enigma's variable components. After the electric current has passed through the plugboard, it enters the rotor assembly by the entry wheel (Eintrittswalze). The entry wheel connects the plugboard to the rotor assembly; the Germans wired the entry wheel to the keys in alphabetical order (Wilcox 2006).

Once the current has passed through the entry wheel, it enters the right-most rotor and continues through the remaining rotors. The rotor assembly usually held three rotors (sometimes four) positioned on an axe. Each rotor is circular and formed from hardened plastic or Bakelite. The rotors are marked with the Roman numerals I, II and III indicating the type of rotor, not its position in the assembly. Each rotor is capable of carrying out a monoalphabetic substitution cipher. With only one rotor, a solution to a ciphered message would be simple. The Enigma machines used at the time of the Polish attack had three rotors, which could be placed in the machine in any order (Christensen2007). The use of multiple rotors allowed the Enigma machines to implement a polyalphabetic substitution cipher, thereby multiplying the strength of its encryption.

On one face of each rotor are 26 fixed contact points with the opposite face containing 26 spring-loaded contact points. The internal wiring of each rotor connecting the contact points is accomplished with insulated wires set in an irregular configuration inside a cylinder. When the three rotors are placed on their axel and positioned in the machine, the contact points on each rotor face line up with the contact points on the opposite rotor allowing the current to flow through. These input and output contacts are the second of Enigma's variable components allowing each rotor to be placed in 26 ways.

The third variable component of Enigma is a ring with either 26 letters or numbers inscribed on its perimeter. The letter ring is etched with a notch, which controls the rotation or "step" of the rotor to its left. For instance, when a key is pressed the right-most rotor moves forward 1/26th of a rotation. When 26 keys have been pressed, the middle rotor will move forward 1/26th of a rotation. After 262 keys have been pressed, the left-most rotor moves forward 1/26th of a rotation. The left-most rotor also has a notch but there is not another rotor to step and the current is passed on to the reflector. In addition to controlling the stepping motion of the rotors, the letter ring is positioned with respect to the internal wiring of the rotors. This means that each contact point corresponds to a letter on the letter wheel. Since the letter wheel controls both the stepping action and is placed with respect to the internal wiring of the rotors then the stepping action provided by the notch is also moving with respect to the wiring.

The fourth variable Enigma component is the finger wheel. The finger wheel has 26 serrations around its edges allowing the operator to turn the letter wheel to a specified starting position. The finger wheels protrude slightly from the top so the machine can be adjusted even when the machine cover is closed. The characters on the letter wheel can also be viewed through small windows beside the finger wheels. Which three characters should be visible through the windows at the beginning of a message was also defined by the assigned code books and is called the ground setting (Rejewski 1980).

The Reflector
German: Umkhrwalzen

To the left of the rotor assembly on the same axel is a non-rotating half drum (reflector) with 26 contact points; which can be moved toward or away from the rotors with a lever. The reflector "bounces" the current back through the components to the lightboard by a different route than it came by. The reflector is the component that enables Enigma to be capable of both encryption and decryption without changing any of the components (Perry 2010).

When a key is pressed on the keyboard a corresponding ciphertext character lights up on the lightboard.For example, if we pressed the letter 'C' on the keyboard and its cipher opposite is 'F' then when we press 'F' we will get back 'C'. This mirror action of the characters is the job of the reflector; this action allows the Enigma machine encryption as well as decryption capabilities. The electric current passes through the rotors, bounces off the reflector and back through the machine in opposite direction. A small and sometimes exploitable tendency of the Enigma was that if the letter 'A'was pressed, onewould receive a ciphertext letter pair for every letter in the alphabet except 'A'. In other words, 'A'would never map back to itself (Rejewski 1980).

We are now ready to discuss the mathematics of the Enigma in terms of its components. We will discuss which components add to the security and which can be eliminated when determining the practical security of Enigma.

Mathematics
Analysis of the Cryptographic Strength Lent by Each Element

The Enigma has five variable components that add to its large keyspace. The components in the table below are multiplied together forming the theoretical keyspace of Enigma. The German's trust in Enigma was based on the large numbers of possible alphabets that it was able to generate. In order to solve an enciphered message, the analyst must find a pattern in the ciphertext message. This is simple as long as only a few alphabets are used and you have a large message, or a collection of small messages all scrambled in the same way. Enigma generated a new alphabet for every letter in the message; this meant that an analyst could not use frequency analysis to try to decipher a pattern in the message.

When researchers want to calculate how much strength is lent to an encryption by a component,they are calculating the number of different alphabets that could possibly be created by each piece. In other words, each component's activityadds up to the encryption process. The Germans relied solely on the theoretical keyspace of Enigma, which is constructed and calculated in the following way:

First, the number of combinations of possible plugboard connections are calculated. The plugboard has 26 different sockets and a maximum of 13 cables are available. Since the cables are dual-wired, each cable takes up two slots on the board.

The second variable component to consider is the rotor contacts. Each rotor has two faces with 26 contact points; the contact points on one rotor line up with contact points on the rotors on either side, connecting different routes for the current to follow through the rotor assembly. It is necessary to calculate how many possibilities are to align the contact points when using three rotors.

Since each rotor has twenty-six input and output contacts, then there are 26! (26 factorial) different ways to connect each rotor. However, the placement of each rotor subtracts one possibility of placement from the next rotor. In other words, the first rotor has 26! different ways it can be arranged, the second rotor has 26! – 1 possible arrangements and the third rotor holds 26! – 2 possible arrangements.

We can write these as a product to find the maximum possible rotors when we are using a set of three in our assembly as follows:

(26!)(26! – 1)(26! – 2) = 65, 592, 937, 459, 144, 468, 297, 473, 480, 371, 753, 615, 896, 841, 298, 988, 710, 328, 553, 805, 190, 043, 271, 168, 000 .000, different possible ways toposition the rotors with respect to their contact points.

The third variable component to be considered is the position of each letter ring. The operator positioned the letter or alphabet ring such that for each rotor in the machine one letter would show through a small window on the top. If there were three rotors then the operator would choose three different letters and the alphabet ring would be turned so that the chosen characters appeared through the windows. Since there are twenty-six letters or characters on each ring and we only need to choose one of each then our calculation for different alphabet ring positions is simple:

26 x 26 x 26 = 26^3 = 17,576, possible settings for all three rotors.

To account for the stepping action of the rotors (the fourth variable component) it is known that the rotor can be placed in 26 different ways, since each time a key is pressed the right-most rotor will step or move forward one position. However, only two of the rotors cause any stepping action to occur since the left-most rotor is connected to the reflector, which does not step. The calculation for the possible settings with respect to the stepping notch becomes:

26 x 26 = 26^2 =676 different settings.

The final variable component multiplying the keyspace of Enigma is the reflector. The reflector is half of a rotor with twenty-six contact points. The reflector waswired such that when the first wire is connected to the first contact then the next wire had one less contact (25) to choose from, the second 23 and so on.

$$25 \times 23 \times 21 \times 19 \times 17 \times 15 \times 13 \times 11 \times 9 \times 7 \times 5 \times 3 \times 1 = 7{,}905{,}853{,}580{,}625$$

To obtain thetotal theoretical keyspaceeach of the variable components is multiplied as follows.

(Plugboard settings) x (Rotor Orders) x (Stepping Notch) x (Letter Ring) x (Reflector)

The above calculation gives a value of approximately 3 x 10^{115} different possible settings of variable Enigma components. Using this value as the theoretical keyspace of Enigma,it is understandable why the machine was assumed to be secure. But the Germans were unable to analyze the practical keyspace of Enigma, which would prove a fatal shortcoming.

Practical Keyspace

To talk about practical keyspace of Enigma the ciphering action of the alphabets as they move through the machine will be examined. The diagram below represents Rejewski's functional circuit of Enigma.

While Enigma's large keyspace generated many alphabets and eliminated the possibility of pattern finding using frequency analysis on a single message, it could not account for German procedures adding depth of their own accord. The problem came from the first six ciphertext letters sent as a preamble to every message. These six letters contained the message key needed by the receiving operator to decrypt the message.

The operator chose three letters to set the alphabet ring on the rotors. These three letters would be enciphered twice,and then sent over radio channels. He immediately recognized this redundancy measure and began working with these first six letters. Rejewski's methods eliminated permutations one by one until the practical keyspacehada much more manageable size. His working keyspace calculations differed slightly from the theoretical keyspace calculations. Rejewski started with four multipliers instead of five,

(Plugboard settings) x (Rotor Orders) x (Ring Settings) x (Groundsettings).

- At the time of the Rejewski attacks, six plugboard cables were in use giving 100,391,791,500 different plugboard combinations (Rejewski 1980).
- Only three rotors were used that could be arranged in the machine in six different ways.
- Only the right and middle rotors contributed to the encryption giving 26^2 = 676 possible ring settings.
- Since all three alphabet rings on the rotors are always manipulatable, we have 26^3 possible groundsettings.

These settings gave Rejewski a starting practical keyspace of 7,156,755,732,750,624,000 possible settings.

To commence the analysisthe behavior of the components during the first six key pressesare analysed.

During the first twenty-six key presses the middle and left-most rotors do not move. This means we can eliminate the action of those rotors in our sample of the first six key presses.

The plugboard contributes the most cryptographic strength to Enigma and is the largest multiplier in the keyspace. According to Kuhl's Recreation of Rejewski's Catalogue, "Rejewski realized that when determining the rotor setting, the effect of the plugboard could be ignored." This eliminates the possible plugboard setting from thepractical keyspacealso.

The action of the middle, left-most rotor and the plugboardhas been, therefore, eliminated from the practical keyspace calculation. The rotor order and the groundsettings are left as multipliers. Working with only these two variables the value of:

(Possible Rotor Order) x (Possible Groundsettings)

$(3!) \times (26^3) = 105,456$, is obtained as a practical keyspace.

In summary, Rejewski started with a practical keyspace of 7,156755,732,750,624,000 and reduced it to 105,456 for the preamble (first six letters) of every message.

The purpose of Enigma was to generate a large number of alphabets and use these alphabets in order to each encipher one letter out of a message. If used properly this measure would have handled the problem of depth. Depth occurs when successive messages transmitted using the same message key allow the analyst to collect a large sample of frequency statistics. From the gathered sample, the analyst can try to deduce a pattern to the permutations of alphabets in the messages. However, because Enigma had such a large keyspace, finding a pattern would require such a large sample that any attempt to find a pattern would take a too large extent of time.

The flaw that reduced the keyspace was the transmission and reception of the preamble containing the settings. The operators set up the Enigmas as prescribed by the codebook and then chose three letters to set the alphabet ring; the operator would push these three letters on the keyboard twice and then transmit them over radio channels. For example, if the operator chose the letters BCE, the operator would set the alphabet ring so these letters appeared in the windows on top of the machine. The operator would then type BCEBCE on the keyboard and would receive the ciphertext characters for these three letters.

Rejewski named the letters in the preamble of the message A, B, C, D, E, and F. Suppose the letters BCEBCE produce the ciphertext LMQPWF. Rejewski would not know the message key; he would know that L changes to P, M changes to W and Q changes to F.

We can write these as compositions as follows;

- (AD) gives us the transposition of L to P.
- (BE) transposes M to W,
- (CF) our last composition transposes Q to F.

If the analyst had a large sample from eighty to one hundred messages all enciphered with the same message key and settings, finding a pattern in the messages would become a viable option. The practical keyspace calculated by Rejewski threw away the daunting statistics of the German theoretical keyspace of Enigma by exploiting the redundancy of the preamble.

Enigma's transpositions occur in pairs. For example, if the 'B' key is pressed causing the 'L' lamp to light, then if the 'L' key is pressed the 'B' lamp will light. This pairing is caused by the reflector and it causes all the permutations A through F of the first six letters to be composed only of transpositions.

First, 'A' is pressed on the keyboard releasing the current. The plugboard initiates the first permutation changing 'A' to 'C' and the current flows into the Entry Rotor. Since the Entry Rotor is wired to the plugboard in the same order as the keyboard, no permutation occurs and the 'C' is passed to the first rotor.

The first rotor causes another permutation and the 'C' changes into a 'D' before passing into the middle rotor. The middle rotor causes the third permutation changing the 'D' into an 'H'. The current is passed into the third rotor causing the fourth permutation from 'H' to 'Q' and passes into the reflector.

The reflector is half of a rotor with twenty-six contact points and causes the fifth permutation; this transposition changes the 'Q' into an 'O'. The reflector bounces the current back into the third rotor where the current follows a new path through the wiring of the rotor initiating a sixth permutation from 'O' to 'M'.

The current travels back into the middle rotor undergoing another permutation (seventh) from 'M' to 'V'. The current passes back into the first rotor changing 'V' to 'X' (eighth permutation). The current undergoes no permutation as it passes through the Entry Rotor once again and enters into the plugboard.

The final permutation of the letter occurs in the plugboard resulting in 'A' being changed into the ciphertext letter 'L'. In the graphic below, we can clearly see each change (permutation) of the letter caused by moving through a component.

If we collected a set of at least eighty messages all enciphered with the same message key, the following analysis of the permutations can be completed.

Consider the following example of a set of three preambles (Rejewski1980.

Let

Set A: dmqvbn
Set B: von puy
Set C: pucfmq

be the three sets of preambles of three different messages. In set A we observe that 'd' changes into 'v'; set B shows 'v' into 'p' and set C shows 'p' into 'f'. We can separate the three sets into compositions AD BE CF.

This gives us the cycles:

- (dvpf) for AD
- (mbou) for BE
- and (qnyc) for CF.

These three sets are called the *characteristic set of the day* and are only partial compositions of the sets of AD, BE and CF. If

more preambles of the 80 messages are analyzed then the complete permutation groups of AD, BE and CF could be composed giving the alphabet for each permutation group.

Rejewski's System of Equations

Rejewski deduced the wiring of the rotors using elementary permutation theorems (Christensen2007). Rejewski's notation labels each component as follows (the following is a summarized example from Rejewski's 1980 publication):

R = Reflector
L = Left-most Rotor
M = Middle Rotor
N = Right-most Rotor
S = Plugboard
Written as
(S N M L R).

Since the reflector causes the inputs to fold back on themselves we write the permutation through the functional circuit of Enigma as

$S\ N\ M\ L\ R\ L^{-1}\ M^{-1}\ N^{-1}\ S^{-1}$.

Due to the stepping action of the right-most rotor or fast rotor, (each time a key is pressed the fast rotor moves forward $1/26^{th}$ of a revolution), Rejewski introduced another permutation P. The permutation P accounts for the change caused by the first rotor. Thew diagram above showed that the rotors cause six of the permutations as the character is enciphered within the Enigma components. With P representing the alphabet generated by the fast rotor, and the rotors being accounted for six times, permutations A through F are produced by the rotors. We raise each to the appropriate subsequent power for each permutation. For example, if we define P the entry permutation as follows:

P = (a b c d e f g h i j k l m n o p q r s t u v w x y z).

Then we can write our permutations A through F as

$A = S\ P\ N\ P^{-1}\ M\ L\ R\ L^{-1}\ M^{-1}\ P\ N^{-1}\ P^{-1}\ S^{-1}$
$B = S\ P^{2}\ N\ P^{-2}\ M\ L\ R\ L^{-1}\ M^{-1}\ P^{2}\ N^{-1}\ P^{-2}\ S^{-1}$
$C = S\ P^{3}NP^{-3}MLRL^{-1}M^{-1}P^{3}N^{-1}P^{-3}S^{-1}$
$D = S\ P^{4}\ N\ P^{-4}\ M\ L\ R\ L^{-1}\ M^{-1}\ P^{4}\ N^{-1}\ P^{-4}\ S^{-1}$
$E = S\ P^{5}\ N\ P^{-5}\ M\ L\ R\ L^{-1}\ M^{-1}\ P^{5}\ N^{-1}\ P^{-5}\ S^{-1}$
$F = S\ P^{6}\ N\ P^{-6}\ M\ L\ R\ L^{-1}\ M^{-1}\ P^{6}\ N^{-1}\ P^{-6}\ S^{-1}$

Multiplying each permutation we can obtain our compositions for AD, BE and CF receiving the following equations.

$AD = S\ P\ N\ P^{-1}\ M\ L\ R\ L^{-1}\ M^{-1}\ P\ N^{-1}\ P^{3}\ N\ P^{-4}\ M\ L\ R\ L^{-1}\ M^{-1}\ P^{4}\ N^{-1}\ P^{-4}\ S^{-1}$

$BE = S\ P^{2}\ N\ P^{-2}\ M\ L\ R\ L^{-1}\ M^{-1}\ P^{2}\ N^{-1}\ P^{3}\ N\ P^{-5}\ M\ L\ R\ L^{-1}\ M^{-1}\ P^{5}\ N^{-1}\ P^{-5}\ S^{-1}$

$CF = S\ P^{3}\ N\ P^{-3}\ M\ L\ R\ L^{-1}\ M^{-1}\ P^{3}\ N^{-1}\ P^{3}\ N\ P^{-6}\ M\ L\ R\ L^{-1}\ M^{-1}\ P^{6}\ N^{-1}\ P^{-6}\ S^{-1}$

The following table of preamble settings is taken from Christensen's paper titled Polish Mathematicians Finding Patterns in Enigma Messages.

The above-cited quote by Rejewski that given a large enough sample, all of the letters of the alphabet will appear in the letters of the preambles, is supported by the table.

Analyzing the A and D letters, for the permutation AD have a full alphabet is obtained, that can be, thereafter, broken into disjointed cycles.

A →A,
B →C, C → B,
F →K, K →X,X → G,G → Z,Z → Y, Y →O,O →D,D → V,V →P,P →F,
H →T, T →E, E →I, I →J, J →M,M →U, U →N, N →Q, Q →L, L →H,
R →W, W →R, S →S,

For the composition AD we have two 10-cycles, two 2-cycles and two 1-cycles.

AD = (fkxgzyodvp)(hteijmunql)(rw)(bc)(a)(s)

The ciphertext alphabet for the composition AD is

The same happens for BE and CF permutations by repeating the above steps. Using this logic, each alphabet needed to decrypt an Enigma message could be deduced.

Conclusion

The confidence Germany had in the Enigma machine can be explained by the large key space it had therefore the theoretical odds of being broken were negligible. This confidence led, in the end, to their demise in both World Wars despite the fact that it was known already after WWI that the German encryption system had been broken by the Allies, therefore it was far from being perfect.

Theoretical odds are not practical odds. In practice, the Allies had many resources to help them crack Enigma, from captured machines and codebooks to perspicacious guess work in some cases. Had Germany switched to a different encryption method during the war instead of adding more parts on the existing framework, the outcome might have been completely different.

The groundbreaking work performed by the Polish would allow encryptions to be read and machine doubles to be built. Ultimately, the failure of Enigma came from its operating procedure: the double encipherment of the daily key provided patterns. Codebooks helped fill in unknowns and others variables, such as the effect of the plugboard, were eliminated entirely once an analysis of the permutations was complete. In one algebraic move the keyspace contributed by the plugboard was entirely reduced. One by one, each part was limited to its practical contribution. Subtractions continued until the theoretical keyspace of 7,156755,732,750,624,000 possible alphabets was reduced to a much more manageable size of 105,456 possible alphabets.

The understandably motivated Polish gave the Allied cryptographers a head start before WWII. In spite of the

continual upgrade and additions the encrypting machine suffered, the system had been broken and no real barrier could be placed against the succesfull exploitation of the system's flaws.

"Hindsight is 50/50" and cryptography moved on, creating larger key spaces and better equipment capable of processing billions of permutations, more creative attacks evolving to meet the challenge every time. Nonetheless, human error is still, more too often, held responsible of the various encrypting systems' breaks.

ACKNOWLEDGEMENT

I would like to thank the following people for their help completing this paper and continuous encouragement. Professor Dagan, who is an awesome teacher! This paper is the result of his Introduction to Number Theory class. I would like to thank my wonderful fiancé Seth Copeland for all his support. My math tutor of five years and friend of ten, Thomas Mizell for always saying, "That is a nice fact, but what does it mean?" Anthony DemicoDelby, for putting up with my constant formatting errors and questions and did not mind keeping me company during late nights of scribbling. The Lawrence Tyree Library and the Martin Luther King Jr. Library for help with documentation and additional search options. Especially Jenna Miller, who gave great advice on citations, databases, and formatting.

REFERENCES

Allen, Keith. (Winter, 1998), *Sharing Scarcity: Bread Rationing and the First World War in Berlin, 1914- 1923.* Oxford University Press, Journal of Social History, Vol. 32, No.2 pg. 371-393. Web.Accessed: 21/07/2012 05:23. Stable URL: http://www.jstor.org/stable/3789666.

Army Security Agency.(1946), *European Axis Signal Intelligence in World War II as Revealed by TICOM Investigations and Captured Material, Principally German.* Department of Defense.
Declassified Material, 2012. DOCID: 3560816

Bennett, Jeffrey O., Briggs,William L. *(*2002) *Using and Understanding Mathematics A Quantitative Reasoning Approach, Second Edition*. New York: Pearson Education, Inc. Print.

Christensen, Chris.(2007)*Polish Mathematics Finding Patterns in Enigma Messages.*Mathematics Magazine.Vol. 80, Iss.4. 247- 273. Print.

Copeland, Jack B. (2004), *The Essential Turing: Seminal Writings in Computing, Logic, Philosophy, Artificial Intelligence, and Artificial Life, plus The Secrets of Enigma*. Clarendon Press, Oxford University Press. 2004. Print.

Deutsch, Harold.(2006),*The Historical Impact of Revealing The Ultra Secret*.US Army War College, 2006.
Unclassified Document, 2006. DOCID: 3827029

Finch, George A.(1930),*The Settlement of the Reparation Problem.* American Society of International Law, The American Journal of International Law. Vol. 24, No.2 , Apr. 1930, pg. 339- 350.

Gunnells, Paul E. (2004), *The Mathematics of Cryptology.*University of Massachusetts, Amherst.Web.
http://www.math.umass.edu/~gunnells/talks/crypt.pdf

Jache, R. Wagoner, T.A. (2009), *The GEE System V: Weaknesses in German Security, TOP SECRET DINAR.* Department of Defense, National Security Agency: Center for Cryptologic History,
Declassified Material, 2009. DOCID: 3565451

Knapp, Thomas A. (1979),*Alfred Hugenberg: The Radical Nationalist Campaign against the Weimar Republic by John A. Leopold*. The University of Chicago Press, Book Review, 1979. The Journal of Modern History, Vol. 51, No.4 (Dec. 1979), pg. 851-853
Accessed: 21/07/2012 04:46 Stable URL: http://www.jstor.org/stable/1877206.

Kozaczuk, Wladyslaw. (1984), *Enigma: how the German Machine Cipher Was Broken and How It Was Read by the Allies in World War Two*. University Publications of America. Print.

Kuhl, Alex. (2007) *Rejewski's Catalog.*Taylor and Francis Group LLC.Cryptologia.Vol. 31. 376- 331. Web.
http://www.alexkuhl.org/research/RejewskisCatalog.pdf

Kozaczuk, Wladyslaw. (1984), *Enigma: how the German Machine Cipher Was Broken and How It Was Read by the Allies in World War Two*. University Publications of America. Print.

Kvetkas, William T. (2003),*The Last Days of Enigma.* Department of Defense, National Security Agency: Center for Cryptologic History, 2003.
Government Release, 2007. DOCID: 3101787

Large, Christine. (2002)*Some Human Factors in Codebreaking.*NATO/ OTAN.Web.
http://www.fas.org/irp/eprint/large.pdf

Larson, Roland E., Hostetler, Robert P., Heyd, David E. (1993), *Precalculus, Third Edition*. Toronto: D.C. Health and Company. Print

Maier, Charles S. (1984), *The Vulnerabilities of Interwar Germany*. The University of Chicago Press, The Journal of Modern History. Vol. 56, pg. 89-99.
Accessed: 21/07/2012 05:38. Stable URL: http://www.jstor.org/stable/1878182

Miller, Ray A. (1995), *The Cryptographic Mathematics of Enigma*.Taylor and Francis Group LLC.Cryptologia.Vol. 19, Iss.1. Pg. 65-80. Web
http://www.nsa.gov/about/_files/cryptologic_heritage/publications/wwii/engima_cryptographic_mathmathema.pdf

Mowry, David P. (2003),*German Cipher Machines of World War II*. Department of Defense, National Security Agency: Center for Cryptologic History. Web.
http://www.nsa.gov/about/_files/cryptologic_heritage/publications/wwii/german_cipher.pdf

Mowry, David P. (2010), *The Breaking of Geheimschreiber*. Department of Defense, National Security Agency: Center for Cryptologic History. Web.
http://www.nsa.gov/public_info/_files/crypto_almanac_50th/The_Breaking_of_Geheimschreiber.pdf

Mowry, David P. (2009), *The Cryptology of the German Intelligence Services.*Department of Defense, National Security Agency, 1989.
Declassified Material. DOCID: 3525898

National Security Agency. (2008),*The German Cryptologic Effort 1918- 1945.*Department of Defense, National Security Agency.
Declassified Material, 2008.

Perry, David. (2010) *The Enigma Code.*NSF-VIGRE at UC Davis.Video Lecture.UC Davis and NSA. http://www.math.ucdavis.edu/research/vigre/outreach/mathfest

Quist, Arvin S. (2002), *Security Classification of Information, Volume 1. Introduction, History, and Adverse Impact.*Oak Ridge Classification Associates, LLC.Web.
http://www.fas.org/sgp/library/quist/index.html

Rejewski, Marian. (1980)*An Application of the Theory of Permutations in Breaking the Enigma Cipher.*ApplicacionesMathmeticae. Vol. 16, Iss.4.Web.
http://cryptocellar.web.cern.ch/cryptocellar/enigma/rew80.pdf

Rejewski, Marian.(1982),*Mathematical Solution of the Enigma Cipher.*Taylor and Francis Group LLC.Cryptologia.Vol. 6.Iss.1. Web.
http://www.tandfonline.com/doi/abs/10.1080/0161-118291856731

Rijmenants, Dirk. (2010), *Enigma Message Procedures Used by the Heer, Luftwaffe and Kriegsmarine.*Taylor and Francis Group LLC.Cryptologia.Vol.34. Iss.4.Web.
http://dx.doi.org/10.1080/01611194.2010.486257

Schmitt, Bernadotte E. (1923),*The World Crisis. By Winston Churchill.*The Academy of Political Science, Book Review, 1923.Political Science Quarterly. Vol. 38, No.4 ,pg. 690-692
Accessed: 21/07/2012 05:45 Stable URL: http://www.jstor.org/stable/2142492

Tucker, Spencer C., Roberts, Priscilla Mary,(2005),*World War I: A Student Encyclopedia*. ABC-CLIO. Pg. 1716- 1717, Print.

Vestergaard, Erik. (2008), *Enigma: The Mathematics Behind the Solution of Enigma.*Henderslev.Web.
http://www.matematiksider.dk/enigma/enigma_math.pdf

Weisstein, Eric W. (2002), *CRC Concise Encyclopedia of Mathematics, Second Edition.*Chapman and Hall. Print.

Wilcox, Jennifer. (2006), *Solving the Enigma: History of the Cryptoanalytic Bombe.* Department of Defense, National Security Agency: Center for Cryptologic History.