The Impact of the Allied Cryptographers on World War II: Cryptanalysis of the Japanese and German Cipher Machines

Katelyn Callahan

December 14, 2013

Abstract

Throughout history, cryptography has played an important role during times of war. The ability to read enemy messages can lead to invaluable knowledge that can be used to lessen casualties and secure victories. The Allied cryptographers during World War II had a major impact on the outcome of the war. The Allies' ability to intercept and decrypt messages encrypted on the Japanese cipher machine, Purple, and the German cipher machine, Enigma, empowered the Allies with a major advantage during World War II. Without this advantage, the war may have had a different end result.

1 A Brief Introduction on Cryptography

Cryptography is the art and science of secret communication [4]. It involves sending a message in such a way so that only the intended audience should be able to read the message with ease. Cryptography has affected many parts of history, including the outcome of World War II.

Steganography is the earliest known form of secret communication, which involves hiding the existence of a message, not the meaning of it [4]. An example of concealing a message can be found in ancient China. A sender would use a messenger whose hair would be shaved off, then the message would be tattooed to the messenger's head. Once the hair grew back thick enough, the existence of the message was concealed. The messenger was then free to travel to the destination to deliver the message. Once there, the messenger would shave his head again so that the message could be read by the intended recipients. This type of secret communication provides little security to a message, since if a message is found, the meaning is known immediately [4]. Consequently, a more secure system was needed to ensure the meaning of a message was not revealed to a potential eavesdropper.

Cryptography, hiding the meaning of a message instead of its existence, is a more secure way of sending a message. In order to send a secret message using cryptographic techniques, one would start with the message that is to be sent, called the plaintext [5]. Before encoding, the sender and receiver agree on the algorithm, the rules by which the message is encoded, to use in order to ensure that both parties can read the message. These rules include the type of cipher that is used and the specific way in which the cipher is used, called the key. Now, the sender uses the key to encode the message. The encoded message is referred to as the ciphertext. Next the encoded message is sent to the receiver. Once the receiver obtains the message, he or she can decipher it by using the decryption key to convert the ciphertext back to the plaintext, and then read the message [5].

An unintended person, who does not know the key, might intercept the message and try to break the cipher. This process is called cryptanalysis [4]. It is always assumed that the type of cipher used in encoding a message is general knowledge, and is known to the person trying to attack the system. The security of a cryptosystem relies on a combination of the strength of the cipher and the key. The more secure the key, the harder it will be for an intruder to decrypt the ciphertext [5]. New ciphers develop when the existing ones have been broken, or when the ciphers no longer seem secure enough for their purposes. The following basic ciphers influenced the development of the cipher machines used by Germany and Japan during World War II.

2 Ciphers that Influenced Cryptosystems Used During World War II

One type of cryptosystem that influenced World War II cipher machines was transposition, which dates back to the fifth century B.C.E. It involves moving all the letters in a message to a different position [4]. If a message was 7 letters long, there would be 7! ways to rearrange the message, that is there are 5040 different ways to rearrange the letters. The longer the message, the more possible ways exist for the message to be encrypted. Unless the sender and receiver agreed on a systematic way to encrypt the message, a trial and error approach could take hundreds of years to exhaust all of the possibilities, depending of the length of the message [4]. By itself, a transposition cipher is not extremely secure. Although it would take a long time to exhaust all possible solutions, a systematic approach from a cryptanalysis could take relatively little time to decrypt the message. However, when used in combination with a different type of cipher, transposition could add security to the cryptosystem [3].

Another influential cryptosystem was the substitution cipher, which involves replacing each letter in the plaintext with a different letter or symbol in a systematic way [4]. One of the most basic types of substitution ciphers is the shift cipher. This cipher is a substitution cipher in which each letter of the alphabet is shifted to a single new position, determined by a key length. A specific example of a substitution cipher is the Caesar shift cipher which shifts each letter three spaces to the right [4]. Each letter is shifted by the following table:

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

This cipher was used by Julius Caesar during his reign as emperor from 49 B.C.E to 44 B.C.E. He used it to send secret messages during his conquests [3]. Caesar shift cipher has become the name commonly used to describe any simple shift cipher. Each letter in the plaintext is encrypted to the corresponding letter in the ciphertext [4]. There are only 26 different ways to encode a message using the Caesar shift cipher, however encoding a to A would only reproduce the original message. Since there is a small, finite number of possible keys, the simplest way to decrypt the message would be by a brute force attack, checking each different key until the ciphertext has been deciphered back to the plaintext [5].

Instead of using a table with letters, a simple shift cipher can be completed using modular arithmetic [5]. First, we assign a numerical value to each letter with 0 representing a, with 1 representing b, and we continue this process up to the letter z. The following chart shows the numerical representation of each letter:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

For the encryption process with a shift length of k, we take the numerical value of each letter of the plaintext, p, and use modular arithmetic to obtain the ciphertext, C, with the following process:

$$C \equiv p + k \bmod (26).$$

For example, to encrypt "Kahn" with a shift of 13, the encryption process is $C \equiv p+13 \bmod (26)$. For example, to encrypt the first letter k, we use the numerical representation found in the above table, 10, in the encryption formula: $C \equiv 10 + 13 \equiv 23 \bmod (26)$. Hence the first letter of the ciphertext would be X. To encrypt the remaining letters, the process is repeated,

$$a \to C \equiv 0 + 13 \equiv 13 \bmod (26) \to N$$

$$h \to C \equiv 7 + 13 \equiv 20 \bmod (26) \to U$$

$$n \to C \equiv 13 + 13 \equiv 26 \equiv 0 \bmod (26) \to A$$

Thus the cipher text reads $XNUA$. To decrypt a message, this process would be reversed; that is, $C - k \equiv p \bmod (26)$. Solving for p yields $p + k \equiv C \bmod (26)$. That is $p \equiv C - k \equiv C + (26 - k) \bmod (26)$. Hence, the decryption key for any message that uses a simple shift cipher is $26 - k$. A Caesar cipher does not have to be shifted by a specific number of letters. Instead, the plaintext could be shifted according to some formula, if the sender and receiver agreed upon it.

A more advanced type of shift cipher is the Vigenére cipher. This method uses many different shifts to encode the plaintext [4]. To start encrypting a message, the sender and receiver agree on a key word or phrase. For example, suppose the keyword is *cillies*. The first letter in the plaintext would be encrypted by the shift that shifts a to c, so the letter is shifted by two, or $C \equiv p + 2 \bmod (26)$. The second letter is now shifted by 8 places, or $C \equiv p + 8 \bmod (26)$, a shift corresponding from a to i. This process continues. Note that the key word, *cillies* is only seven letters long. Thus the eighth letter would be shifted according to the first letter in our key word. This process would continue until all of the plaintext has been encrypted. To encode "Bletchley" using the codeword *cillies*, observe the following encryption process,

plaintext	b	l	e	t	c	h	l	e	y
numerical representation (p)	1	11	4	19	2	7	11	4	24
keyword	c	i	l	l	i	e	s	c	i
k	2	8	11	11	8	4	18	2	8
$p + k$	3	19	15	30	10	11	29	6	32
$C \equiv p + k \bmod (26)$	3	19	15	4	10	11	3	6	6
Ciphertext	D	T	P	E	K	L	D	G	G

Thus, the ciphertext would read $DTPEKLDGG$. This cipher has more security than a simple shift cipher. In the Vigenére cipher, it is possible for two different letters in the plaintext to be encrypted to the same ciphertext letter. The strength of the system comes from the length of the key and the ability of the cryptanalyst ability to deduce the key. The Vigenére cipher is harder to break using a trial and error approach since each letter of the plaintext has 26 possible shifts (it is possible, although not widely common, that the key word is as long as the plaintext) [4]. In the example above, the plaintext repeats the letter e twice, but each e is encrypted to a different letter. By using different shift ciphers in the same message, a letter will not necessarily be encrypted to the same ciphertext letter each time it appears in the plaintext. Because of the different shift ciphers used to encode a single message, an attack by frequency analysis would most likely be of little help in decrypting the message. Also, repeated letters in the codeword does not lessen the strength of the cryptosystem. However, the weakness with the Vigenére cipher is in its cyclical nature. Since the message is encoded using a certain length keyword, after a certain number of letters have been encrypted, the specific shift cipher used will repeat, creating a cycle. This repetition creates the weakness of the cipher. Once a cryptanalysis has figured out the length of the cycle, an attack by frequency analysis can be performed [4].

A block cipher is a type of cipher that encrypts letters in blocks [5]. Each block is encrypted according to the other letters in the block. A type of block cipher is the ADFGX cipher. This cipher was used during World War I by German cryptographers. The ADFVG block cipher labels each row and column of a $5X5$ grid with the letters A, D, F, G, X and the grid is then filled with the letters of the alphabet according to some algorithm, and i and j are placed in the same block. Each letter of the plaintext is encrypted to the label of its row and column. A key word is chosen, and the key word labels the columns of a new grid formed by the encrypted letters. The columns of this grid are then rearranged into alphabetical order. The ciphertext is found by reading down the columns of the matrix.

For example, the first step in encrypting *mathematics* with the keyword *playfair*, is to create a 5×5 grid with row and columns labeled as *A, D, F, G, X*:

	A	D	F	G	X
A	a	o	b	p	c
D	q	d	r	e	s
F	f	t	g	u	h
G	v	ij	w	k	x
X	l	y	m	z	n

To encrypt $mathematics$ using the grid, note that m is in row X and column F. Thus m is encrypted to XF. Next, a is in row A and column A, and a is encrypted to AA. By continuing the process for the remaining plaintext, *XF AA FD FX DG XF AA FD GD AX DX* is obtained. Now, the new grid is formed by labeling the columns with the key:

P	L	A	Y	F	A	I	R
X	F	A	A	F	D	F	X
D	G	X	F	A	A	F	D
G	D	A	X	D	X		

Next, the columns are arranged in alphabetical order:

A	A	F	I	L	P	R	Y
A	D	F	F	F	X	X	A
X	A	A	F	G	D	D	F
A	X	D		D	G		X

The ciphertext is obtained by reading down the columns, *AXADAXFADFFFGDXDGXDAFX*.

To decrypt a message, this process would be reversed. If the key word is known, then the ciphertext can be separated into a certain number of groups depending on the length of the keyword. Then a grid can be formed by writing the letters of the ciphertext down the columns. The label of each column is the letters of the keyword in alphabetical order. The columns are then arranged so that the keyword is reproduced. The letters in the grid are then written down, going across the rows. These letters are grouped into pairs, each pair corresponding to a letter in the ciphertext. The 5×5 grid that was used to encrypt the message needs to be found. Then the intersection of the row of the first letter in the pair with the column labeled with the letter of the second is the corresponding plaintext letter for each pair.

A frequency attack would not be very useful, since the ciphertext contains only five different letters. Instead, the key and the 5×5 grid needs to be reproduced in order to decrypt a message. A cryptographer wishing to break the system could try analyzing the letters and trying to come up with patterns between encrypted messages.

All of these cryptosystems have been broken. By combining the strengths of each type of cipher while improving on their weaknesses, a new cryptosystem can be developed that is more secure than any previous one. Each of the cryptosystems discussed above influenced the development of the Japanese and German cipher machines, Purple and the Enigma.

3 American Cryptographers Overcome The Japanese Cryptosystem, Purple

3.1 Purple

During World War II, Japan's major source for encrypting messages was an electrical machine the Americans called Purple. The cipher machine, Purple consisted of a plugboard, keyboard, four rotors, and a coding wheel. The plugboard interchanged the wirings of any two letters by use of a cable. The four rotors would rotate after a certain number of letters had been encrypted, according to the settings of the coding wheel. To encrypt a message, the operator would first plug in the cables to switch the appropriate letters according to the instructions for that day. The operator would then set the coding wheel so that the rotors would rotate at the appropriate time. The last step in setting up the machine was to turn each rotor to its starting position. The operator would type the plaintext into the keyboard, and Purple would print out the ciphertext [3].

3.2 American Cryptographers' Attack on Purple

It was the American cryptographers that were successful in breaking Purple. The cryptographers spent months analyzing patterns in intercepted ciphertext. They grouped letters in the ciphertext by the expected cycle lengths of that letter. From this, the cryptographers were able to deduce certain letters of the plaintext that were logical. Experts in Japanese would then fill in some of the missing letters to form words in the plaintext. From their studies, the cryptographers were able to design a machine that would encrypt a message exactly the same as Purple did. Using this machine, they could now decrypt whole parts of a message in a shorter amount of time then it took the cryptographers by hand. After a year and a half, the American cryptographers were able to completely decrypt an entire message that was encrypted using Purple [3].

Occasionally, Japanese cryptographers would encode their messages before encrypting them using Purple. This process was only used on messages that needed the highest level of security. It took the American cryptographers an additional year after breaking Purple to read a message that was encoded and then encrypted using Purple. Through careful analysis of the messages and studying patterns between them, the cryptographers were able to read even the most secure Japanese messages [3].

William Friedmen was the leader of the American cryptographers that broke Purple. He spend all his free time analyzing the messages since he was obsessed over cracking the cipher machine. It is said that he could not eat or sleep until the cryptosystem had been broken. Because of his obsession with success and the thought of the national consequences that would follow if his teamed failed, his physical and mental health declined. He spent over three months in a hospital recovering from a mental breakdown. He returned to work as soon as possible, although not given the same task load [3]. The work that the cryptographers did during World War II had a major impact on the war. The cryptographers realized that failure was not an option since the fate of their country was at stake.

3.3 Advantages of Breaking Purple

In June 1942, the Japan government sent a message to its troops describing the plan of attack at Midway. A small number of Japanese troops were to distract the enemy by attacking a group of nearby islands, forcing the Allied troops way from the island of Midway; therefore, providing Japan with an easy victory [4]. The message was intercepted and deciphered by the American cryptographers and they warned the Allied troops of the plan. In order to avoid suspicion that Purple had been broken, the troops pretended to leave the island, making Japan think the Island of Midway was vulnerable. As soon as Japan began to attack, the troops turned around and initiated a surprise assault [4]. The United States military was able to stop Japan from taking over the island, and assured themselves a surprise victory for the Allies. This was the Allied forces first major victory in the Pacific. It gave the Allied forces a secure base in the Pacific, and kept Japan from pushing forward towards the western coast of the United States and Hawaii. From this location, the Allied forces were able to keep pushing forward towards Japan.

Another example of the advantage that the Allied forces gained from being able to read Japanese messages encrypted on Purple was the discovery of the location of a significant Japanese military leader. In 1943, the Americans intercepted a message stating the exact location of the Japanese Commander-In-Chief of the Air Force, Isoruko Yamamoto. The American military was able to take full advantage of this knowledge without letting Japan know that their cryptosystem had been broken. The U.S. Air Force was able to locate and shoot down Yamamotos plane. This feat was significant because he was thought to be responsible for the attack on Pearl Harbor and the attack on Midway. One of the major figures in the Japanese military had been killed because of the United States ability to break Japans cryptosystem, and thus read their encrypted messages [4].

4 Allied European Cryptographers overcome the German Cryptosystem, The Enigma

"I do not imagine that any war since classical times, if ever, has been fought in which one side reads consistently the main military and naval intelligence of the other."

Stuart Milner-Barry

4.1 Enigma

The Enigma machine was the main source for secret communication for the Germans during World War II. Enigma's encoding process started by typing a letter of the plaintext into the keyboard. An electrical current would be shot through the three rotors, hit the reflector board and be sent back through the rotors in the reverse order, and illuminate a lightbulb that was labeled with the corresponding letter that would be written down to achieve the ciphertext [4]. A plugboard was installed to switch the wiring of any two letters. For example if a and w were plugged together on the board, when a was pressed, it would be encoded by the machine as if w was pressed. When w was pressed on the keyboard, the machine would encode the letter as if a was pressed. The plugboard acted like a transposition cipher and provided additional security to the encrypted messages [1]. For added complexity, each rotor would shift its position by one place after a certain numbers of keys had been pressed, creating a cipher similar to the Vigenére cipher. A ring was positioned on the left and middle disk that determined how many keys needed to be pressed before the next rotor would shift one place [6]. This shift in position ensured that a specific letter was not always encrypted the same; therefore, making an attack by frequency analysis nearly impossible.

The Enigma was invented by the German Arthur Scherbius in 1918. When he first tried to exclusively sell his machine to the German military, he was turned down [6]. The German military thought that the system they previously had was secure enough for their purposes. Due to this decline, Scherbius redesigned a version of the machine for commercial use. It was not until the early 1920s that the military saw the benefit that came with using this cryptographic machine [4]. Germany's previously used cryptosystem, the ADFGX cipher, was broken by Allied cryptographers during World War I. Germany was not aware of the Allied cryptographers achievements, and the German cryptographers thought they still possessed a secure system. After the war ended, Winston Churchill, the Prime Minister of England, announced that his troops had captured Germany's codebooks containing the list of keywords and algorithms to find the 5×5 grid used to encrypt all German messages. His cryptographers were able to read all messages that were intercepted from Germany. German cryptographers realized that they needed a new cryptosystem; one that would not be compromised if their codebooks were captured. The Enigma became Germany's main source for encrypting and decrypting messages. With the discovery of radio waves and the invention of the telegram, Germany and the rest of the world were able to send and receive hundreds of encoded messages a day.

The German government created and distributed code books and copies of the Enigma to the military. The code books contained the initial setting of the rotors and plugboard for each day. Each message sent would start with a three letter keyword that was not encoded. This keyword would indicate the rotational position of each rotor [1]. The next six letters were encrypted and contained a three letter code word repeated twice, to ensure accuracy. When the intended audience received a message, the operator would type the next six letters after the key into the machine, revealing the code word [4]. This code word would inform the operator on the specific initial position of the rotors to decrypt the rest of the message. For example if the code word was ADF, the operator would rotate the first rotor so that A was positioned at the top. He would position the second rotor to read D, and the third to read F. Once the positions were set, the operator could type in the rest of the message, recording the corresponding lights to each key stroke.

4.2 Allied Cryptographers Attack On The Enigma

The Germans thought that their machine was unbreakable, and for a time this seemed to be true. France was the first country to make an attempt to break the Enigma. The cryptographers thought that by purchasing a commercial Enigma they could gain insight on how the German military was enciphering their messages [4]. This proved to be of little help since the commercial version contained four rotors and no plugboard. In 1931, France finally received the help that they needed. First, Hans-Thilo Schmidt, a German man who worked with the German cryptographers, sold France documentation and keys of the Enigma machine [6]. Second, in 1931, an agreement between France and Poland was made stating that if Polish cryptographers continued their efforts to crack the Enigma messages, the French government would give over any knowledge they acquired on the Enigma. When this agreement was made, the Polish government decided not to hand over the information they had acquired about the wiring of Enigma to their cryptographers [4].

Marian Rejewski, who was Polish, was one of the men that was given the task of discovering how the machine was wired. After months of analyzing numerous intercepted German messages, Rejewski deduced a complicated equation that could explain how the machine worked. However, his equation had too many unknown variables to be of much use [6]. Once the government was sure that he could make no further progress with his equation, Rejewski was given the documentation of the Enigma that the French had turned over. It still took months to solve for some of the unknown variables [4]. Finally, he was able to figure out how the wirings of the rotors in the Enigma worked. To determine the overall wiring of the machine, Rejewski tested his best educated guesses. First, he assumed that the machine worked by sending an electrical current from the plugboard to the keyboard. After many failed attempts to decipher German messages, he decided that this was not the wiring of the Enigma. He then decided to try a few more different possibilities. Through this guess and check method, Rejewski eventually discovered that the Enigma's plugboard was wired alphabetically to the rotors. He also determined how the current flowed through the rest of the machine [6]. Now that the Polish cryptographers knew the internal wirings of the machine, they were able to build replicas to help decipher intercepted messages.

Having a replica of the machine was not enough to crack the Enigma, although it was the first step in this process. The next step was determining the initial setting of the machine so the Allies could easily read all of the intercepted messages [1]. This task was by no means a small one. Note that the plugboard had 26 different sockets, one for each letter of the alphabet. Since each cable connected was inserted into two sockets, the number of cables that could have been used ranged from 0 to 13. Let c represent the number of cables being used. There are two properties to consider: the number of cables that are used; that is the number of letters that are selected to be switched, and the number of ways there are to plug the cables into the sockets [1]. Order does not matter when choosing what sockets are to be plugged with the cables. For example, if $c = 2$, and a, f, g, h were selected, this would be the same as choosing if f, h, a, g. The number of ways to choose $2c$ sockets with c cables from 26 sockets is given by $\binom{26}{2c}$. Next, consider the number of ways to plug in the c cables into the selected $2c$ sockets. Note that there are $2c$ ways to connect the first end of the first cable, which leaves $2c - 1$ possible connections for the other end. The second cable's first end has $2c - 2$ ways to connect to the plugboard, leaving $2c - 3$ possible connections for the remaining end. This process continues until only one socket remains. There is only one way to plug the last cable into the remaining socket, since it does not matter what end is plugged in first. Thus the total possible ways to plug in c cables is given by

$$(2c - 1)(2c - 3)(2c - 5)....(5)(3)(1).$$

For example, assume that two cables are being used and that the letters a, f, g, k have been chosen to be switched. Note that if the first cable was connected to a the second end of the cable could be connected to f, g, or k. Once one of these connections was picked, say a is connected to f, then there is only one way to plug in the last cable, g is connected to k. Thus, the total number of ways to connect 2 cables is $3 = (2(2) - 1)(2(2) - 3)$ To find the total number of possible setting for the plugboard, the number of different ways to choose $2c$ sockets and the number of ways to plug in the c cables are multiplied together [1]. Hence, the total number of possible settings for the plugboard when c cables are used, denoted by N, is

$$\begin{aligned}
N &= \binom{26}{2c}(2c - 1)(2c - 3)(2c - 5)....(5)(3)(1) \\
&= \frac{26!}{(26 - 2c)!(2c)!}(2c - 1)(2c - 3)(2c - 5)....(5)(3)(1) \\
&= \frac{26!}{(26 - 2c)!}\frac{(2c - 1)(2c - 3)(2c - 5)....(5)(3)(1)}{(2c)!} \\
&= \frac{26!}{(26 - 2c)!}\frac{1}{(2c)(2c - 2)(2c - 4)....4(2)} \\
&= \frac{26!}{(26 - 2c)!(2^c)(c)(c - 1)(c - 2)....(3)(2)(1)} \\
&= \frac{26!}{(26 - 2c)!(c!)(2^c)}.
\end{aligned}$$

Note that the following table is a list of all the possible number of settings for c cables:

c cables	total number of settings
0	1
1	325
2	44,850
3	3,453,450
4	164,038,875
5	5,019589,575
6	100,391,791,500
7	1,305,093,289,500
8	10,767,019,638, 275
9	53,835,098,191,875
10	150,738,274,937,250
11	205,552,193,096,250
12	102,776,096,548,125
13	7,905,853,580,625

Since the number of cables being used by the German military was not known to the Polish cryptographers, the sum of the possible settings for each number of cables, where $0 \leq c \leq 13$, gives the total number of settings for the plugboard. Thus, the true number of possible setting of the plugboard is

$$\begin{aligned}
\sum_{c=0}^{13} \frac{26!}{(26-2c)!(c!)(2^c)} &= \frac{26!}{(26-2(0))!((0)!)(2^0)} + \frac{26!}{(26-2(1))!(1!)(2^1)} + \frac{26!}{(26-2(2))!(2!)(2^2)} \\
&+ \frac{26!}{(26-2(3))!(3!)(2^3)} + \frac{26!}{(26-2(4))!(4!)(2^4)} + \frac{26!}{(26-2(5))!(5!)(2^5)} \\
&+ \frac{26!}{(26-2(6))!(6!)(2^6)} + \frac{26!}{(26-2(7))!(7!)(2^7)} + \frac{26!}{(26-2(8))!(8!)(2^8)} \\
&+ \frac{26!}{(26-2(9))!(9!)(2^9)} + \frac{26!}{(26-2(10))!(10!)(2^{10})} + \frac{26!}{(26-2(11))!(11!)(2^{11})} \\
&+ \frac{26!}{(26-2(12))!(12!)(2^{12})} + \frac{26!}{(26-2(13))!(13!)(2^{13})} \\
&= 1 + 325 + 44850 + 3453450 + 164038875 + 5019589575 \\
&+ 100391791500 + 1305093289500 + 10767019638375 + 53835098191875 \\
&+ 150738274937250 + 205552193096250 + 102776096548125 \\
&+ 7905853580625 \\
&= 532,985,208,200,576.
\end{aligned}$$

Next consider the number of possible initial positions for the three rotors. Each rotor would have a different configuration of 26 letters along the notches, and the Allied cryptographers had no way of knowing how the letters were positioned according to the others. Thus there were 26! possible rotors that the Germans could have used [1]. However, the Allies did know that the Enigma only held three disks. Since each disk was different from the others, there were $26!$ possible rotors for the first position, $26!-1$ possible rotors for the middle position of the Enigma, and $26!-2$ different possible rotors for the leftmost position. Hence the number of possible rotors is given by

$$(26!)(26!-1)(26!-2) \approx 6.56(10)^{79}.$$

Each of the rotors, left, center, and right, had 26 possible ways to be placed in its individual position in the machine. This corresponds to the 26 notches on each of the rotors. Thus once the rotors have been arranged there are $26^3 = 17,576$ possible ways to position them [1]. Next, consider the rings positioned on the rotors that controlled the shift of each rotor. The ring on the first rotor caused the middle disk to shift after a certain number of keystrokes, and the ring of the middle disk caused the rightmost disk to shift after a certain number of encrypted letters [4]. Since there were 26 different notches on a rotor, there were 26 different ways for each ring to be positioned [1]. Hence, the total number of combinations due to the shifting on the rotors was $26(26) = 676$. Lastly, consider the reflector. Once an electrical current passed through the three rotors, it would hit the reflector at one of its 26 faces. If the current was sent back through the same face, the electrical current would pass through the same path back through the rotors and light up the same key pressed, unless the letter was connected on the plugboard [1]. Hence, each face was connected to another face. The total possible settings should be the same as having 13 cables for the plugboard, since all 26 letters of the alphabet and 26 different faces are switched [4]. Hence, the reflector added 7,905,853,580,625 more possible configurations to the Enigma. Since all of the possible setting of the individual parts of the Enigma have been calculated, the total number of settings of the Enigma is calculated by multiplying together the total number of settings of the plugboard, rotors, rings, and reflector [1]. Note that

$$(532,985,208,200,576)(6.56(10)^{79})(17,576)(676)(7,905,853,580,625) \approx 3(10)^{114}$$

Thus there were approximately $3(10)^{114}$ different settings of the Enigma that the Allies would need to check if they had wished to break the machine through a brute force attack [1].

The extreme amount of possible settings for the Enigma that the Germans had to work with would suggest that the Germans had a system that was nearly impossible to break. However, the Germans did not use this machine to its full potential. The German military usually kept the rotors in the same position relative to each other for up to three months [4]. If the Allied cryptographers were able to determine the position of the rotors, they would not have to recalculate this for at most three more months.

Some of the German cryptographers tended to use the same code over multiple messages. For instance, if the first three letters of a message read HIT, then the next six letters of the plaintext would likely read $LERLER$, making the keyword $Hitler$. One of the cryptographers that would encode the plaintext messages written by German officers commonly used the name $Cillie$ as his codeword. If an intercepted message started with CIL, the Allied cryptanalysis would then deduce that the next six letters of the plaintext should be $LIELIE$ [4]. Once the replicas of the Enigma machine were built, the machine could run through numerous settings of the machine until the one that would decrypt the ciphertext back to the codeword was found.

In 1939, Poland knew Germany would soon invade the country. Thinking that it would no longer be safe to continue making progress with the Enigma cipher, the Polish cryptographers and government decided to turn over all of the knowledge that they had acquired about the Enigma, along with the replicas they had built to the French and British governments [4]. The British government immediately hired the top minds in the fields of mathematics, science, and engineering to work on deciphering Germany messages at a facility at Bletchley Park. Alan Turing created plans to simplify the Polish machine. He believed that the machine would run more efficiently if it was built to check patterns in an assumed text [6]. Because many of the intercepted messages contained $cillies$, the Allied cryptographers could assume what the first three decrypted letters should be on the Enigma. With this knowledge, the cryptographers only needed to check settings that encrypted the first three letters to the assumed key. Instead of running through hundreds of thousands of possible settings, the cryptographers would need to test a small number of settings to determine the key [6]. Once this was accomplished, the cryptographers could change the settings on the replica, and decrypt the rest of the message.

The machine Alan Turing designed, known as the Bombe, worked by running through hundreds of possible settings simultaneously [6]. The rotors in Bombe would spin at high speeds checking for all positions that would encode the three letter encrypted key to the three letter assumed key. The rotors would stop spinning once a possible match was found. The operators of the machine were members of the Womens Royal Naval Service [6]. Once they had noticed a part of the machine had stopped spinning, they would write down the settings of the machine and reset the rotors so that Bombe could continue to run through numerous settings to find another position that encrypted to the correct letters. Over the length of the war, Britain built 210 of these machines and distributed some of them to other Allied countries [6].

The German Navy had stricter rules and regulations than the German Army and Air Force using the Enigma. First, most naval messages were encoded using a codebook before being encrypted on Enigma [6]. Second, instead of using three rotors, the naval Enigma had the possibility of using eight different rotors for the three positions [4]. Very few of the messages sent contained $cillies$, and the Germans tried to ensure that no messages repeated whole sections of text, therefore making it hard for the Allied forces to find patterns between different messages [6]. Thus the British cryptographers could not find a common assumed text to test on their Bombe. Deciphering the messages by hand was nearly impossible, and extremely time consuming. The Allied forces were not able to read German Navy messages until they captured the codebooks and the rotors [6]. In 1941, a German crew in fear of sinking, abandoned ship and forgot to destroy the codebook, instructions, and key lists that were aboard. The British military was also able to capture all eight rotors, along with the Enigma machine with that days settings still intact [4]. The German Navy never suspected that their information had been captured and believed that none of the Enigmas secrets had been stolen. Using this information, the British cryptographers could easily read all intercepted Navy messages. However, the key list soon ran out of entries [6]. To ensure that they would not be in the dark about naval message for the remainder of the war, British cryptographers used the codebook, key list and instructions to create additional Bombes that could run through the settings of this unique machine [4]. The key list ran out before the Bombe was able to be completed. For a time, the Allied forces were once again in the dark about the German Navys plan. Once the Bombe was built, the British cryptographers could decipher almost all of the German intercepted messages within two day [6].

4.3 The Advantages of Breaking the Enigma

The messages that the Allied forces were able to intercept led to major victories that contributed to the outcome of the war. The military could not use all of the information that they received from the cryptographers. If the Allied forces were able to defeat the Axis at every turn, and continuously dodge all attempts at attack, the German military would become suspicious that their cryptosystem had been broken. The Allied cryptographers would no longer be able to read the messages if the Germans changed their cryptosystem, and the Allied forces would be once again on their own. However, the Allies did use some of the information to their advantage.

Navy messages, when deciphered provided useful information to help the Allies gain and keep control of the seas [4]. The Allied forces had the necessary information to keep their ships safe, letting the fleets know when and where enemy ships would try to attack. They knew the location of most German U-boats and were able to sink almost twenty-five percent of the U-boats during one summer of the war [6]. The Allied forces also saw a rapid decline in the amount of successful attacks on Allied ships. The German High Commander was not suspicious with the sudden turn of the war. His confidence in the cryptosystem was too great, and he believed that the Enigma was unbreakable [4]. Instead, he attributed the sudden success of the Allied forces to information gained from a prisoner of war. He was convinced that one of his captured men had given away information on major German naval plans. The ability to keep Germany from taking over the Atlantic gave the Allied forces control of the seas.

In 1944, the Allied troops planned to invade the beaches of Normandy, France and take back Western Europe. This task was greatly helped by the British cryptographers. A message was intercepted and deciphered stating the exactly location, and in what capacity the Axis troops were positioned [3]. With this information the Allied forces were able to better prepare their attack, and inform their troops where to position themselves.

All of the cryptographers that worked on breaking the Enigma were sworn to silence [4]. They were not allowed to talk about any of their work, even years after the war ended [6]. During the war, the cryptographers at Bletchley park did not know the extent to which the military used the information that they deciphered. They understood the work they were doing was important, but they were never given information on how their successes with the Enigma helped the Allies win the war. Even thirty years after the war ended, Britain still kept the success of its cryptographers a secret from the rest of the world [6].

The Allied forces overcame remarkable odds in breaking the Enigma machine. The Germans compromised their cryptosystem by not using the Enigma to its full potential: “Had the cipher machines been used properly - without repeated message keys, without $cillies$, without restrictions on plugboard settings and scrambler arrangements, and without stereotypical messages which resulted in cribs - it is quite possible that it might never been broken at all” [4]. It is said that the war was shortened by as much as two years because of the efforts by the Allied cryptographers in breaking the Enigma and their ability to decipher German messages.

5 Cryptographic Influences In The Modern World

Once a cryptosystem is broken, cryptographers learn from its weaknesses and try to create a new cryptosystem that is either a more advanced version or a new way of encryption is created all together. Germany and Japan realized that their cipher machines, the Enigma and Purple, had been compromised, and that they needed new cryptosystems to use for encrypting their messages. The cryptosystems that developed in response helped further influence the cryptosystems in use today.

Cryptography as a science has evolved since World War II. Cryptography is no longer used solely by nations, but is now involved in most people's everyday life. An example is cryptography's role in keeping online banking secure. The information is encrypted as an attempt to deter a third party from stealing millions. Cryptography still plays a major role in matters of national security. Although, because of its secret nature, the extent to which the government uses cryptography or the exact ciphers and cryptosystems it uses will not be known until after the system has been broken.

Although the Enigma is not still used to encrypt messages, it has recently made a reappearance. A machine went up for auction in London on October 29, 2013. It was manufactured in 1944 and used by the German military to encrypt their messages. There are not many Enigmas still intact today. The German government destroyed their copies to ensure that the machines were not captured by unintended parties. Also the codebooks and wiring blueprints were either burned or lost throughout World War II and the years to follow. The machine being auctioned off is one of the few remaining Enigmas that still contain all of its original parts. It sold for $91,839 [2].

References

[1] A. Ray Miller. The Cryptographic Mathematics of Enigma, Center for Cryptologic History, indent National Security Agency, 2011.

[2] "Bonhams : A Rare Three-rotor German Enigma Enciphering Machine, 1944,." Bonhams. N.p., 29 Oct. 2013. Web. 14 Nov. 2013. ¡http://www.bonhams.com/auctions/20774/lot/58/¿.

[3] Kahn, David. The Codebreakers: The Comprehensive History of Secret Communication from Ancient times to the Internet. New York: Scribner's and Sons, 1997. Print.

[4] Singh, Simon. The Code Book: The Science of Secrecy From Ancient Egypt to Quantum Cryptography. New York: Anchor, 1999. Print.

[5] Trappe, Wade, and Lawrence C. Washington. Introduction to Cryptography: With Coding Theory. 2nd ed. Upper Saddle River, NJ: Pearson Prentice Hall, 2006. Print.

[6] Wilcox, Jennifer. Solving the Enigma: History of the Cryptanalytic Bombe, Center for Cryptological History, National Security Agency, 2006.