It has been suggested that Graeme Base was influenced by the ENIGMA codes during World War II. For older learners, this aspect of the war could be studied in conjunction with social studies classes. Below is a summary:

THE ENIGMA MACHINE: Codebreaking and Secret Weapons in World War II

By Bill Momsen

1926-1939

Two words describe the German WWII fighting machine successes: organization, and communication. Their lightning "blitzkrieg," which allowed them to roll over Europe almost unopposed, was a well-coordinated operation employing panzers (tanks) and Stukas (dive bombers). At sea, their efforts were aimed at cutting England's supply line from North America by well-directed submarine "wolf pack" attacks on convoys. For communications, the Germans relied almost entirely on messages sent by radio. These messages could be heard, of course, by anyone equipped with receiver.

To ensure that the enemy would not intercept vital information, they used an electro-mechanical device called Enigma to encode the data. They believed that even if the enemy were to capture a machine, it would be useless unless both sender and receiver were also in possession of the same "key" which described how the message was encoded. The Poles proved them wrong.

The Germans used different radio frequencies and keys for messages sent to their various units. This ensured that messages meant for the Luftwaffe (Air Force) were not readable by the Kriegsmarine (Navy). By assigning different keys to different units, communication could be directed to the appropriate unit. Not only would there be no point in a submarine decoding a message meant for a panzer unit, but some ultra-secret messages (for example to the SS) were confidential.

What Went Wrong?

Enigma codes could have been unbreakable, at least with the methods available at the time, had the machine been used properly. The biggest mistake the Germans made was their blind belief in the invincibility of Enigma. Procedural errors in using the machine, combined with occasional operator laziness, allowed the Poles and, subsequently the British, to crack the "unbreakable" codes.

In addition to the general key, a "message key," unique to each message, was part of the transmission. Each army unit had two enigma operators, one to work the machine, the other to write down the lit-up letters on the lampboard. Often these men were not properly trained in the use of the machine. They were allowed to pick their own message keys, at times making some very poor choices.

The navy had better safeguards; only officers were allowed to set up the machines. The message keys were specified and carefully chosen to minimize the possibility that they could be deduced by the code breakers. The code lists were printed with water-soluble inks and kept under lock and key at all times. The navy's extra precautions were effective; the Allies were unable to crack the naval codes until two years after they had broken the army's.

Communication

To send information from one place to another some form of communication system is necessary, whether it be by voice, waving flags, firing guns, over telegraph wires, or by radio. As early as 170 B.C. Polybius described a system using a number of torches placed in various positions to represent letters of the alphabet.

There are three reasons to use codes for message transmission: 1) to make transmission more efficient; 2) in case the transmission medium cannot carry voice (the telegraph can only transmit dots and dashes); and 3) to hide the meaning of the message from prying eyes. An example of the first is a scheme to save toll charges on international telegrams (which are charged by the word) by having a single word represent a whole sentence.

There are two methods of preparing a message for transmission: 1) Coding, in which words or phrases are represented by symbols, and 2) Encipherment, in which letters in a plain text message are represented by other letters or characters according to some scheme. In *Superencipherment*, the message is first coded and then enciphered, making it doubly hard to crack. *Cryptology* is the two-part science of *Cryptography,* encoding; and *Cryptanalysis*, the breaking of codes.

Codes

A code relies on a list or book of phrases and words, which might be:

0001	alert
0002	all gone
0003	ammunition
0004	antitank
0005	attack
0005	attention

Thus, “antitank ammunition all gone” would appear as 0004 0003 0002. Solutions to this type of message are greatly complicated if the code groups are not arranged alphabetically, of course. This type of system was used extensively by both sides during WWI. The code was compromised if the codebook was captured. In fact, this is precisely what happened when in 1914 the German warship *Magdeburg* went aground in the Baltic. Due to a series of errors, the Russians were able to recover the codebook and the Imperial German Naval code was an open book. Worse yet, the Germans did not know (or chose not to believe) that their code was no longer secure.

Another method involved printing a number of “one time pads.” Each page had an abbreviated code printed on it. After each use, one page was torn off and discarded. The Germans soon realized that the size of their forthcoming military operation precluded printing up the number of pads that would have been required.

Ciphers

The simplest of all ciphers uses mono-alphabetic substitution. The alphabet is written out, and under it, a second alphabet consisting of all the letters at random:

a b c d e f g h .... z
ZRNFTQMA ....

In this example, the word “face” is encoded as QZNT. The recipient refers to his copy of the cipher to turn the message back into plain text. Note that with this scheme, “face” will always be encoded as QZNT.

Mechanical Ciphering Machines

Mechanical ciphering rings and rotating cylinders have been with us since antiquity. L. B. Alberti described a cipher disk in the 15th century A.D. Thomas Jefferson invented a ciphering device consisting of a number of rings on a common shaft. All of these were purely mechanical. The first electro-mechanical rotor device was invented almost simultaneously by three men. Edward Hugh Hebern, in the United States, was the first, coming up with a machine in 1918 which was used by the U.S. in World War II. In 1919 Hugo Alexander Kock in the Netherlands invented another version, assigning his rights in 1927 to Arthur Scherbius, whose improved model was the basis for the German Enigma. Also in 1919 Arvid Gerhard Damm in Sweden came up with his own machine. Boris Caesar Wilhelm Hagelin bought Damm’s company, and continues to produce improved rotor machines in Switzerland.

The Machine

In 1918 Arthur Scherbius patented a ciphering device which allowed businesses to communicate confidential documents without having to resort to clumsy and slow codebooks. His invention consisted of a number of rotors turning on a common axis. The rotors had the numbers 1 to 26 marked on their edges, which were visible through the front panel of the machine. Thumbwheels connected to each rotor protruded above the panel. The operator could set a "starting position" for each rotor by means of the thumbwheels.

Each rotor was equipped with 26 electrical contacts (one for each letter of the alphabet) on each side. The contacts on one side were randomly connected by wires to the contacts on the other side. An electrical current obtained by pressing a key on a typewriter-like keyboard entered the first rotor on one side, and exited on the other side at the terminal determined by the cross-wiring. Which output terminal was energized depended on both the position of the rotor and its cross-wiring.

If the rotor did not turn, each of the 26 input letters would always have the same encode, determined by the rotor wiring. In the Scherbius machine, however, the first rotor turned 1/26 of a revolution each time a letter key was pressed. Thus, inputting the letter "a" might be encoded as any one of the 26 letters, depending on the rotor wiring and starting position. Typing in a text consisting of nothing but the letter "a" would result in a string of 26 garbled letters, until the rotor returned to the starting position, when the string of garbled letters repeated exactly. But the Scherbius machine had more than one rotor, all connected mechanically like the odometer on an automobile. Transposition with one rotor repeated after 26 letters. With two rotors it occurred after 26 x 26 = 676 letters, with three 26 x 26 x 26 = 17,576. Note that unlike the mono-alphabetic scheme, this is a poly-alphabetic system, using a *different* encoding alphabet each time a key is pressed.

Scherbius' machine was not a commercial success, and in 1918 he offered it to the German Navy, suggesting a seven rotor device (6 billion combinations) or one with thirteen rotors (100 trillion possibilities). Scherbius calculated that even if an enemy possessed 8-rotor machines and messages in both plaintext and cipher, it would require 1,000 operators working 24 hours a day 14.5 years to find the key.

The military at first rejected Scherbius' machine. He and his associates continued to improve the device.

Birth of Enigma

The rotors were modified so they could be removed from the machine. This meant that the rotors (each with different cross-wiring) could be placed in the machine in a different order. Another modification was made to the rotors. A rotatable ring which could be locked into any one of 26 positions was attached to each rotor, marked with the numbers 1 to 26 that had previously been on the rotors. (In the naval model of Enigma, letters were substituted for numbers). The operator referred to a table on the inside of the lid to translate letters into numbers, for example J=10). Instead of an indicator letter representing a particular position of the rotor, the two were no longer related, and the position of the alphabet ring on the rotor had to be known to the decipherer. The notches that caused the next rotor to move ahead one step were moved from the rotor to the ring. Now the rotors' nudge to turn over the next rotor had no relationship to the rotor's transpositions.

When a key was pressed, say "a," electric current from a battery entered the first terminal on the right hand rotor. The current passed from this terminal via the rotor wiring to its output terminal on the left side, exiting perhaps at encoded terminal "P." The current then passed into the "P" terminal of the middle rotor, exiting at the output terminal corresponding to its wiring, say "M." It then proceeded to the "M" terminal on the third rotor, exiting at "V."

Each time a key was pressed, the right hand rotor rotated to a new position. After a given number of keypresses, the second rotor arrived at its "turn over point" and rotated. Likewise with the third rotor. In fact, it was possible for all three rotors to turn at once if each of them were at their turnover positions.

The Umkehrwalze

A further refinement added a fixed "rotor," the *umkehrwalze* (turn around wheel), on the left side which, through its wiring "reflected" the electrical pulses back through the other rotors via a different path. This resulted in reciprocity between encipherment and decipherment; if "a" was enciphered as "X" then "x" would be enciphered as "A." An advantage of this system was that at any given setting a machine could either encipher or decipher. The disadvantage was that if somehow one letter of a message was decoded, a second one would also be known.

With this system no letter could ever represent itself. The final result of this was that the input letter "a" might come out of the scrambler as any one of the 26 letters, for example, "K," *except* "A." This complicated the codebreaking in one sense, but also might speed a solution to the code by showing which possible solutions could be rejected.

The Steckerboard

The German Army Field Enigma. The Germans added another complication to Enigma. They interposed a plug board with 26 jacks and a number of patch cords (usually 6) which could cross-connect any two letters between the keyboard and the rotors. It was located at the very front of the machine. By mixing up these 12 letters before they entered the scrambler, the number of possible encipherments was raised by a factor of 2 to 3 billion, to a staggering 10 quadrillion. If 1000 operators with captured machines tested four keys a minute 24 hours a day, it would take them 900 million years to try them all! The Germans were convinced that their codes were quite unbreakable.

The German keys

Although the Enigma machine was physically modified numerous times as the war continued, as were the methods of using it, it is instructive to examine a genuine early message to see how it was used. The following communication, sent Sept. 21, 1938, appeared in "The Turing Bombe: Was it Enough?" by C. A Deavours and Louis Kruh (Cryptologia, October 1990, Vol. XIV, No. 4, p. 342), furnished them by David Kahn. Although it was transmitted by land line, the procedure would have been the same had it been sent by radio.

A message is to be sent to Army Group Command #2, starting as follows: "Auf Befehl des Obersten ...". Each particular unit on a net (a particular radio frequency) was assigned a "Daily Key" (*Tagesschlüssel*), somewhat of a misnomer, as the interval between when they were changed varied as the war proceeded. The Daily Key contained information as to how the machine was to be set up. The message may be decrypted using any of the Enigma simulators available on the net (see Bibliography), and for this particular message, the settings are:

1. Rotor Order (*Walzenlage*): II, I, III

2. Ring settings (*Ringstellung*): ZWD

3. Plugboard connections (*Steckerverbindungen*): EZ, BL, XP, WR, IU, VM, JO

There were several identifiers *(Kenngruppen)* associated with each key that could be used interchangeably to confound possible codebreakers (e.g. AXPWT, YDTEC, EIHBF, etc.). Any one of the group identified a particular key. Different sets of keys were issued to users on the same net. If the receiving operator intercepted a message including an identifier he did not have, he knew the message was not for him, and could not be decoded.

The first part of the message was in plain text (unencrypted), and contained the sender, recipient, date and time, and how many sections, if the message was broken down into several parts (to make cracking the code more difficult, messages were supposed to be limited to less than 200 characters, although this stricture was not always followed).

The operator picked three letters at random (the "Starting Position", (*Grundstellung*) and set his code wheels to those three letters, FRX in this case. These were also transmitted *en clair*, twice in case there were garbles in transmission. He then picked three more letters at random, AGI for the first segment of this particular message. He typed this triplet (the "Message Key", *Spruchschlüssel*) twice also, but this time it was encoded before transmission. He then typed in the first three letters of the message body. The next five letter group, the identifier, was inserted unencoded. He then proceeded to type in the rest of the message. This will perhaps become clearer when the decoding process is discussed. It should be emphasized that although this method was used in late 1938, the procedures varied widely as the war progressed. More commonly, the Message Key directly followed the Starting Position.

The doubly-enciphered message key was a serious mistake, as it led to a break-in by the Poles. Even worse was the operators' penchant for choosing keyboard diagonals (QAY), AAA, etc. When they were forbidden to do this, they substituted their girl friends' initials or abbreviated obscenities. Although the message key was supposed to be different for each part of a message, they frequently re-used the same letters over and over. This was put to a stop when the war started, and operators were supplied with sheets of randomly chosen three letter groups to be used as message keys, but it was too late - the Poles already had their foot in the door. On May 10, 1940 the double encipherment was dropped, and the message key (AGI) was only typed in once.

The sender set his rotors to FRX, typed in AGI AGI, and lamps HCA LNU lit up in succession. This formed the first part of the encrypted message. He then moved his rotors to the "real" message key, AGI, and typed in the first 3 letters of the message, AUFB which became QKRQ. The identifier AXPWT was dropped in and the rest of the message followed. Thus:

```
AGIAG IAUFB AXPWT EFEHL SDESO BERST EN ...

HCALN UQKRQ AXPWT WUQTZ KFXSO MJFOY RH ...
```

`FRX AGI ptext AGI` (rotor settings used)

```
       AN HEERESGRUPPENKOMMANDO 2=
2109 -1750 - 3 TLE - FRX FRX -          1TL -172=
```

```
HCALN UQKRQ AXPWT WUQTZ KFXZO MJFOY RHYZW VBXYS IWMMV WBLEB
DMWUW BTVHM RFLKS DCCEX IYPAH RMPZI OVBBR VLNHZ UPOSY EIPWJ
TUGYO SLAOX RHKVC HQOSV DTRBP DJEUK SBBXH TYGVH GFICA CVGUV
OQFAQ WBKXZ JSQJF ZPEVJ RO -

2TL - 166 -
ZZWTV SYBDO YDTEC DMVWQ KWJPZ OCZJW XOFWP XWGAR KLRLX TOFCD
SZHEV INQWI NRMBS QPTCK LKCQR MTYVG UQODM EIEUT VSQFI MWORP
RPLHG XKMCM PASOM YRORP CVICA HUEAF BZNVR VZWXX MTWOE GIEBS
ZZQIU JAPGN FJXDK I -

3TL - 176 -
DHHAO FWQQM EIHBF BMHTT YFBHK YYXJK IXKDF RTSHB HLUEJ MFLAC
ZRJDL CJZVK HFBYL GFSEW NRSGS KHLFW JKLLZ TFMWD QDQQV JUTJS
VPRDE MUVPM BPBXX USOPG IVHFC ISGPY IYKST VQUIO CAVCW AKEQQ
EFRVM XSLQC FPFTF SPIIU ENLUW O = 1 ABT GEN ST D H NR. 2050/38 G KDOS +
```

The receiving operator first examined the identifier, AXPWT (third group). If it was not on his list, he would not bother to try decrypting the message. The unencoded "preamble" in this case is:

AN HEERESGRUPPENKOMMANDO 2 =

2109 -1750 - 3 TLE - FRX FRX - 1TL -172 =

The first line reads: “To Army Group Command #2”

The second can be broken down as follows:

2109: The date, Sept. 21

1750: The time, 17:50

3 TLE: This message is in three parts

FRX FRX: The “*Grundstellung*” (starting position of the rotors)

1TL - 172: The first part, comprised of 172 characters

The first six characters, HCA LNU are the twice-enciphered rotor starting positions for the message. Since the Army machine had numbers rather than letters inscribed on the rotors (01=A, 02=B, etc.), the receiving operator was required to first convert FRX into 06 18 24 with the help of a table on the inside cover. He then set his rotors to 06 18 24, typed in HCA LNU, and noted that lamps AGI AGI lit up in turn. He then set his rotors to AGI (01 07 09), typed in the first three characters, skipped the next group of five, and entered the rest of the message.

The second part starts with plaintext 2TL - 166 -, that is, part 2 comprised of 166 characters. The operator set his rotors back to FRX and decoded ZZW TVS as YBE YBE, placed the rotors in this new position, and decoded the remainder of part 2, skipping over TDTEC. He then performed the same operation for part 3. The message was then separated into words:

AUF BEFEHL DES OBERSTEN BEFEHLSHABERS SIND IM FALLE X Z X ZT X UNWAHRSCHEINLICHEN X FRANZOESISQEN ANGRIFFS DIE WESTBEFESTIGUNGEN JEDER ZAHLENMAESSIGEN UEBERLEGENHEIT ZUM TROTZ ZU HALTEN X

FUEHRUNG UND TRUPPE MUESSEN VON DIESER EHRENPFLIQT DURQDRUNGEN SEIN X ABS X DEM GEMAESS BEHALTE IQ MIR DIE ERMAEQTIGUNG ZUR PUFGABE DER BEFESTIGUNGEN ODER AUQ VON TEILEN AUSDRUECKLIQ

PERSOENLIQ VOR X ABS X AENDERUNG DER ANWEISUNG X OKH X GEN X ST X D X H X ERSTE ABT X NR X DREI DREI ZWO EINS X DREI AQT G X KDOS X VOM JULI EINS NEUN DREI AQT BLEIBT VORBEHALTEN X DER OBERBEFEHLSHABER DES HEERES

Certain conventions were observed:

X = Period or word divider

ABS = New paragraph

AQT = /

Q = CH

ZXZT (z.Zt) = “zur Zeit”, “at this moment”, a common German abbreviation.

Applying these corrections, we obtain a final version of the message (in German, of course).

Auf Befehl des Obersten Befehlshabers sind im Falle, zur Zeit unwahrscheinlichen, Franzoesischen Angriffs die Westbefestigungen jeder zahlenmaessigen Ueberlegenheit zum trotz zu halten.

Fuehrung und Truppe muessen von dieser Ehrenpflicht durchdrungen sein.

Dem gemaess behalte ich mir die Ermaechtigung zur Aufgabe der Befestigungen oder auch von Teilen ausdruecklich persoenlich vor.

Aenderungen der Anweisung OKH/Gen/St/D/H Erste Abt Nr. 3321/38 G/KDos vom Juli 1938 bleibt vorbehalten.

Der Oberbefehlshaber des Heeres.

The Poles had one more step - to translate the message into Polish, although it is rendered here in English:

The Commander-in-Chief orders as follows:

In the case of French attacks on the western fortifications, although unlikely at this moment, those fortifications must be held at all costs, even against numerically superior forces.

Commanders and troops must be imbued with the honor of this duty. In accordance with orders, I emphasize that I alone have the right to authorize the fortifications to be abandoned in whole or part.

I reserve the right to make changes to order OKH/Gen/St/D/H 1. Abt. Nr. 3321/38 GKDos of July 1938.

The Commander-in-Chief of the Army.

“Westbefestigungen” (western fortifications) probably refers to the Siegfried Line, which paralleled the French Maginot Line in the west. It was named after a figure in German literature known for his outstanding strength and courage. One-third of Germany’s cement production was going into this fortification by 1938.

Note that most Enigmas had only the 26 letters; numerals had to be spelled out (3321 = DREI DREI ZWO EINS). The longer the message, the greater the likelihood of it being broken, so it was imperative to keep each message as short as possible. In some Navy Enigma-M machines the upper row keys were labeled 1/Q, 2/W, ... 9/0 and 0/P. The start and end of a numeric string was indicated by the letter Y. With this method in use, 3321 = YEEWGY, a saving of 9 characters. For the most part, this method was abandoned at the start of the war, but was used in certain circumstances until 1942.

In the early days multi-part Naval Enigma messages started with FORT (abbreviation for Fortsetzung, continuation) followed by the serial number of the previous part, repeated. One such message indicating that the previous section was part 2330 became FORTYWEEPYYWEEPY.

The Poles

The Poles were keeping a jaundiced eye on their German neighbors in the period between World Wars. During this time all the major powers and some of the minor ones were routinely decoding each other’s messages. The Polish Biuro Szyfrów (Cipher Bureau) was among the best. The team that cracked the Enigma codes was comprised of Marian Rejewski, Jerzy Rózycki and Henryk Zygalski. By the end of the War, 10,000 people with sophisticated computers were decoding Axis messages, which they never could have done without the pioneering work of these three brilliant men.

In 1926 German naval messages suddenly underwent radical transformations, and were no longer decipherable by the Poles. In 1928 the Army dispatches followed suit. By espionage they discovered that the Germans had started to machine-encode their traffic. They purchased a commercial Enigma machine, but it was unable to untangle any of the dispatches.

Espionage

Hans Thilo-Schmidt, originally of a German aristocratic family, had fallen upon hard times. He persuaded his brother, a Lieutenant Colonel in the German signal corps, to give him a job. One of his tasks was to destroy Enigma codes which were no longer valid, which granted him access to information he decided to sell to the French (using the code name Asché. He furnished Gustave Bertrand of the French Intelligence service a booklet detailing the Enigma machine setup procedures. There was no mention of the rotor wiring or information on the keys.

The French puzzled over this information, then consulted with the British, who agreed that it was insufficient to be of any practical use. Bertrand then offered it to Marian Rejewski in Poland who was overjoyed upon receiving even this small crumb. Rejewski asked Bertrand if he could obtain some outdated Enigma keys. The Frenchman relayed this request to Schmidt who readily obliged, and the keys were passed back to Poland.

Solving the Rotor Wiring

The Poles now had:
1) Messages in plaintext.
2) Messages in code.
3) The keys used to convert that plaintext to code.
The only unknown was the rotor wiring. Rejewski was able to set up a set of equations in four unknowns, three of which were known, and solve them for the unknown rotor wiring. The terms of these equations were not simple mathematical quantities, but permutations. Using permutation theory, and Rejewski's original theorem regarding the product of transpositions, 5 successive plaintext letters and their encodes were plugged into the equations. An assumption was made that neither the middle nor slow rotors moved in this period, likely because in 21 cases out of 26 they did not. In this manner the wiring of the right-hand "fast" rotor was determined. (Rejewski's equations and reasoning appear as appendices in Garlinski and Kozaczuk, see Bibliography).

The order in which the rotors were placed in the machine was changed every three months, after which the order was repeated. As each of the different rotors was dropped into the right-hand position, the same analysis was performed, until the wiring of each of the three rotors was known.

The Poles had a replica Enigma machine made, based on the commercial model with the rotors rewired, in great secrecy. They set up the machine according to the code, fed in the encoded message and - out came gibberish! Rejewski checked and re-checked his equations, and was almost ready to give up in despair when he wondered if the wiring from the keyboard to the scrambler was A to A, B to B, etc., unlike the commercial model, which was Q to A, W to B, ... (keyboard order). The machine was re-wired and out came plaintext! The year was 1933, and they now had a functional Enigma replica.

(There are various accounts of how the Poles reconstructed the Enigma. Kahn states that the Poles built a machine by mathematical analysis based on stolen keys and intercepted messages. Winterbotham claims that a Polish factory worker memorized the rotor wiring. Lewin relates that the Poles intercepted an Enigma machine being shipped to the German embassy in Warsaw. Welchman repeats Stevenson's story of an ambushed German truck, its Enigma replaced by a dummy, then set on fire. The evidence, particularly that from the codebreakers themselves, overwhelmingly supports the view that the Enigma replica was reconstructed from mathematical models.)

“Cribs”

Although the Poles now had an Enigma replica, this was only half of what was needed. The machines had been designed so that even if the enemy captured one, it would be useless without the keys. A “crib” is a fragment of plaintext which is known to correspond to a section of code of the same length. The Germans were very helpful in furnishing the Poles with cribs. Many of their messages started with “anx” (“an” = “to” in German, with “x” as a word separator).

The German operators helped the codebreakers no end by selecting message keys like AAA, ZZZ, or QAY (the leftmost diagonal of the keyboard).

Machine Cycles

All Enigma operators used the same daily “net key”, although the “message keys” were different for each transmission. In other words, each message started at a different position in the scrambler cycle. Was it possible to work backwards from the message to find out where it started in the cycle? Although there were 17,576 possible starting positions, the scrambler was not a randomizer; its output was predictable. For example, would it be possible to input “abcdefg” and have the output be “ZNRQXML” at *all* of the starting positions? Obviously not, but it might be possible at one, several or many starting positions.

Rejewski collected a list of the first six letters from all messages transmitted each day. It was known that the first and fourth (1,4), second and fifth (2,5), and third and sixth (3,6) letters of the message key were identical. He was able to construct chains of how the identical letters changed as the scrambler moved each time a letter was entered. He discovered a characteristic cycle that was different for each scrambler position. In 1934 the “cyclometre” was invented, a device consisting of two sets of rotors and reversing drums three letters out of phase, interconnected by switches and lamps, and operated by hand. It took them a year, but the Poles were able to construct a card catalog of the characteristic cycles at each of the 6 x 17576 possible positions (the 6 possible combinations of the 3 rotor placements multiplied by the number of scrambler positions). After that, it took only 20 minutes to look through the card file and discover the daily setting. On November 1, 1937, the Germans changed the umkherwalze wiring, and the card catalog was useless. The cataloging process had to be done all over again.

Zygalski Sheets

It took the Poles less than a year to complete the second card catalog, but on September 15, 1938 the Germans changed their method of enciphering the keys, and the card catalog and cyclometre were useless. The only time the doubly enciphered message key could be used was when, by chance, the 1,4, 2,5 or 3,6 pairs were *identical* (for example PST PWA or RLQ MLZ). A 1,4 pair (called a “female”) occured on average once every 25 messages. The same holds true for 2,5 and 3,6. The chances that a 1,4 *or* 2,5 *or* 3,6 female occurs is about 1 in 8. If 60 messages in the same basic key were available, chances are that one of the females would appear at least once. Since these could only occur at certain positions of the scrambler, and if those positions could be identified, the message could be decoded.

10 sets of “Zygalski sheets” (one set for each of the ten possible rotor positions) were prepared. Each set consisted of 26 large squares of paper (one for each position of the slow rotor), marked at the top and side with letters of the alphabet. Rows represented the position of the of the middle rotor; columns positions of the slow rotor. If a female was possible at some position of the rotors (for example, the “A” sheet of the slow rotor, with center rotor at “M” and the fast rotor at “R”), a hole was laboriously cut at the intersection using a razor blade.

The sheets were placed one by one on top of each other, positioned according to 12 females found in the messages. If, after 12 sheets had been stacked, light shone through all the sheets in one place, a possible key had been found. If not, a different sheet (or set) was selected, and another stacking performed. These settings were tried, one by one, on an Enigma replica.

The Bomby

The methods discussed so far did not identify the actual key, only a number of possibilities, which had to be tried, one by one, on an Enigma replica until the operators' fingers were raw and bleeding. What was needed was a machine to accomplish this task.

The Enigma scrambler was single-ended; one set of terminals served both as input and output. What was needed was a device where certain input terminals could be energized, and as it went through all the possible positions, a second set of terminals monitored to detect a desired output. For example, if it was assumed that the first three letters of a coded message HJQ represented the plaintext anx, input terminals H, J, and Q are energized and output terminals a, n, and x monitored. The machine steps through all cycles until a match is found, and then stops.

Three sets of double-ended scramblers, one machine cycle apart, were driven by a motor. In our example, input terminals H, J, X were energized, and the machine stopped at any occurence of a, n, x. For each test run, 6 bomby were required, one for each of the 6 possible rotor positions.

The machines made a ticking noise as they worked, and stopped when they arrived a solution. The Poles called them *bomby* (plural, "bomba" singular), perhaps from the ticking of the clockwork in a bomb fuse which stopped just before it exploded. Another possibility is that the name came from an ice cream dish they were eating at the time.

With keys given them by the French, and using replica machines they had built, the Polish team of Marian Rejewski, Jerzy Rózycki and Henryk Zygalski were able to decode most German messages. They were particularly interested in radio traffic between German troops training in Russia, a ploy which allowed them to circumvent terms of the Versailles Treaty. However, they never related their results to the French, probably because they feared the Germans would find out that their codes had been compromised and institute new procedures which would nullify their success. The French, puzzled at receiving no intelligence, continued to pass on the keys nevertheless.

The Poles began their efforts when the Germans used only three rotors. Although the keys were out of date, they were able to apply them to a backlog of messages.

Complications

Dec. 15, 1938 the Germans added two new rotors, making five available, although only three were used in the machine at any one time. The Polish resources were severely strained, as now 60 sets of Zygalski sheets and 60 bomby (at a cost of 1.5 million zlotych, about $350,000) would have been required. This, and knowing from intercepts that their country was about to be invaded, persuaded the Poles to share their information with the French and British. The British had decided to take a crack at Enigma codes, but it was too late; the Germans had added complications that made a break impossible. The Poles, having a ten year head start, were able to take advantage of the days when coding methods were simpler, and operators, becoming used to the new system, made some serious mistakes.

July 25, 1939, at a secret meeting in the Kabackie Woods near the town of Pyry, the Poles handed over their complete solution to the German codes, their Enigma replicas and bomby to the dumbfounded British.

Many accounts of the meeting mention a mysterious “Mr. Sandwich”, speculating that he was Stewart Menzies, head of British Intelligence. In an interview with Patrick Beesly (“Who was the Third Man at Pyry”, Cryptologia, II, #2, 324-330) Admiral John Godfrey Director of O.N.I. (Office of Naval Intelligence) disclosed that he had sent Commander Humphrey Sandwith to the meeting. In later interview with Beesly, Gustav Bertrand confirmed that he was indeed Sandwith.

On September 1, Hitler invaded Poland. On the 5th, the codebreakers packed up their Enigma replicas, Zygalski sheets and bomby, and made a run for France. After a mad flight in the company of thousands of others trying desperately to flee the Germans, they made it through Austria to France, but had to destroy all their equipment along the way. The Poles continued their work in France, sharing their work with the British. In fact, the British furnished them with sixty sets of 26 Zygalski sheets, since theirs had been destroyed in the evacuation.

Epilogue

When the Germans occupied the rest of France, the Polish codebreakers fled to England. Only some of them made it. Most were captured by the Germans while attempting to cross the Pyrenees into Spain.

Since it was their brilliant work, turned over to the British, which allowed the Allies to read the German messages, it is hard to believe that the English never allowed them to work as codebreakers on the vital Kriegsmarine (Navy) *Schlüssel-M* traffic, which was not broken until naval rotors VI and VII were captured. Might not Rejewski have been able to employ the same methods in solving the wiring of those rotors that he had so successfully used before?

Was it British arrogance that denied the Poles their due in so many publications once “Ultra” was no longer under wraps? Perhaps not. The secrecy was so tight that most of the British codebreakers could not have known that their work was based on Polish success.

And what of the three men who did so much to shorten World War II? Jerzy Rózycki was lost at sea Jan. 9, 1942, enroute from Algeria to France. Henryk Zygalski decided to remain in England after the War, where he died in 1978. Marian Rejewski returned to Poland, where he died in 1980 at the age of 74. To add injury to insult, at the Yalta Conference in February, 1945, the Communist Lublin Party in Poland was recognized, not the Polish Government in exile in London.

These three men received little monetary compensation for their efforts, not much in the way of promotions, and only a few minor Polish decorations. They merited the highest accolades of all the Allied Nations. Perhaps their satisfaction came from a job well done.

What If?

The British had given up trying to break Enigma codes when the Poles showed them how it could be done. It is quite probable that the codes would not have been broken without their assistance. The Battle of Britain and the Battle of the Atlantic might have been lost, and England forced to capitulate. The Americans would have been denied a staging ground for the invasion of Europe. The War might have dragged on for another two years, with many more millions of lives lost. Far worse, given this respite, Hitler might have developed the atomic bomb and, almost unthinkably, mated it to a three stage intercontinental ballistic missile capable of crossing the Atlantic Ocean.