Lecturas Matemáticas
Volumen **34** *(1) (2013), páginas 85–130*
ISSN 0120–1980

Descifrando Enigma. La Epopeya polaca

Enigma Deciphering. The Polish Epic

José Manuel Sánchez Muñoz
Universidad Politécnica de Madrid, España

Resumen. Este artículo trata la importancia de la desencriptación del Código de la máquina Enigma alemana a manos de los polacos gracias al trabajo analítico de matemáticos como Marian Rejewski, cuyo resultado fue vital para la derrota de los nazis en la 2ª Guerra Mundial, acortando ésta al menos en dos años.

Key words and phrases. Nazis, Mathematics, World War Two, criptology, BS4, Rejewski, Enigma.

Abstract. This article considers the importance of the German Enigma machine code cracking by the Poles through the analytical work developed by mathematicians as Marian Rejewski, which had vital consequences for the Nazi defeat in the Second World War, shortening it by around two years.

2010 AMS Mathematics Subject Classification. 01A

1. Las máquinas de cifrado y Enigma

1.1. El origen de Enigma. Al final de la 1ª Guerra Mundial se produjo la aparición y proliferación de las máquinas de cifrado de rotores. Estas máquinas permitían a los criptógrafos mecanizar el proceso de cifrado polialfabético, pero aumentando enormemente el número de posibilidades de encriptación, haciendo prácticamente inaccesibles las tareas de aquellos que intentaban desentrañar qué se escondía tras los mensajes cifrados con dichos mecanismos. Estas máquinas fueron desarrolladas de forma independiente por varios inventores de diferentes países en un lapso temporal de varios años. La inclusión de varios rotores se produjo con el fin de complicar el algoritmo de cifrado. Este tipo de máquinas daban la posibilidad además de simplificar al máximo su operatividad y funcionamiento. Algunas de estas máquinas se utilizaron ampliamente

durante la 2ª Guerra Mundial, y algunos ejemplos son la Enigma alemana, la máquina púrpura japonesa, o la estadounidense M-209. Casi todos los códigos que se ocultaban tras ellas fueron descubiertos por los enemigos. Una de las que sin lugar a dudas tuvo más impacto mediático por su repercusión y todas las connotaciones que surgieron en torno a ella fue la alemana Máquina Enigma.

La primera máquina de cifrado de rotores fue inventada en los EE.UU por Edward Hugh Hebern (1869-1952). Entre 1912 y 1915 patentó varios dispositivos de cifrado como un teclado de cifrado y dos máquinas de escribir eléctricas conectadas con un cableado de 26 conexiones para el cifrado monoalfabético automático. Hebern construyó su primera máquina cifrado en 1917, la cual tenía únicamente un rotor que podía ser extraído y cambiar su orientación con el fin de ser utilizado para cifrar y descifrar mensajes. Hebern mejoró su máquina implementándola con nuevos rotores hacia 1921, cuando solicitó su patente y fundó la Hebern Electric Code Company. El criptoanalista estadounidense William Friedman, que conseguiría romper la japonesa máquina púrpura, mejoró el diseño original de Hebern con la invención de la SIGABA. La máquina de Hebern tenía un rotor que giraba y mantenía fijos los otros para 26 caracteres de un mensaje, haciéndola vulnerable al criptoanálisis. La SIGABA tenía una rotación irregular, lo que hizo que fuera una de las pocas máquinas de cifrado cuyo código no fue roto durante la 2ª Guerra Mundial. Hebern únicamente vendió una docena de máquinas antes de llegar a la bancarrota, lo que provocó su entrada en prisión por haber defraudado a sus inversores.

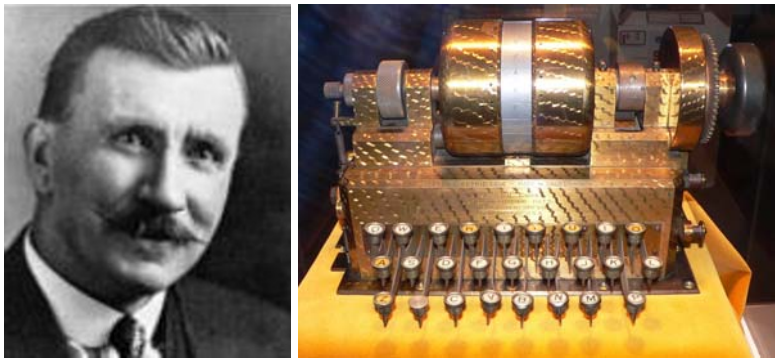

Fig. 1. Edward Hugh Hebern (izq.) y Máquina Hebern (drcha.).[1]

La segunda máquina de cifrado de rotores fue inventada en 1918. Ese año el ingeniero alemán Arthur Scherbius y su íntimo amigo Richard Ritter fundaron la compañía *Scherbius & Ritter* (más tarde rebautizada en julio de 1923 como *Chiffriermaschinen Aktien Gesellschaft*), una innovadora empresa

[1] http://ciphermachines.com/types.html

de ingeniería que cubría un amplio rango de invenciones. SCHERBIUS era el encargado de lo que hoy denominamos I+D, buscando continuamente nuevas oportunidades. Uno de sus proyectos preferidos era sustituir los inadecuados sistemas manuales de criptografía empleados en la 1ª Guerra Mundial por una codificación mecánica y automática que mejorara las posibilidades de cifrado, aumentando la cifra de permutaciones posibles, y simplificando en gran medida la labor del emisor del mensaje cifrado. SCHERBIUS había estudiado ingeniería eléctrica en Hannover y en Múnich, y desarrolló una pieza de maquinaria criptográfica que era esencialmente una versión eléctrica del disco de cifras de Alberti. Nadie podía sospechar que el invento de origen civil de SCHERBIUS, se convertiría en el más temible sistema militar de codificación de la historia.

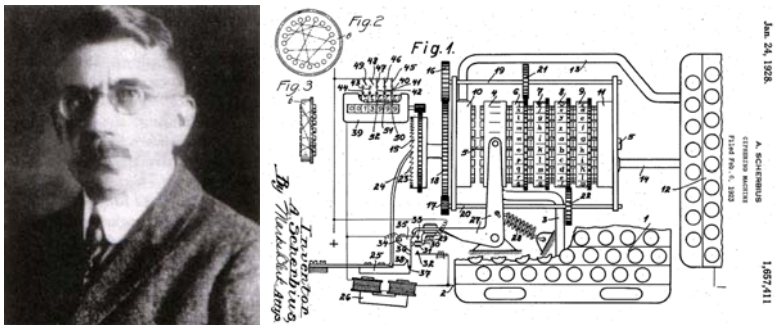

FIG. 2. A. SCHERBIUS y Patente americana (US - 1.657.411) de Enigma (A. Scherbius, 24 Enero - 1928).[2]

El 23 de febrero de 1918, SCHERBIUS solicitó la primera patente de la máquina comercial Enigma, con el fin de crear una máquina que mantuviera en secreto las principales transacciones de información en el mundo empresarial. Enigma era relativamente fácil de transportar y muy potente, rápida y cómoda a la hora de generar mensajes cifrados. La primera versión comercial, conocida con el nombre de Enigma-A, fue puesta a la venta en 1923. A esta primera versión le siguieron tres modelos comerciales. El modelo Enigma-C vio la luz en 1926, siendo su principal característica su liviano peso de 11,8 kg frente a los 49,9 kg de sus antecesoras. El modelo Enigma-D se convirtió en el más relevante, y el que tuvo verdadero éxito comercial. A pesar del origen comercial de Enigma, la armada alemana en febrero de 1926, y posteriormente el ejército el 15 de junio de 1928, adquirieron su propia máquina Enigma, adaptándola y cambiando su fisonomía acorde a sus necesidades, como la inclusión del clavijero en 1930, o la modificación de las conexiones del cableado de los rotores con el fin de aumentar el número de posibilidades de cifrado y complicar más aún si cabe su criptoanálisis. Sin duda éste era un síntoma claro de que ambos estaban

[2] http://news.sciencenet.cn/htmlnews/20085151025471820659.html y http://http://en.wikipedia.org/wiki/Arthur_Scherbius

contraviniendo todas las directrices especificadas en el Tratado de Versalles ya que la intención principal de estas adquisiciones era la protección de sus comunicaciones en primera instancia y el rearme como fin último. El ejército alemán comenzó a utilizar el diseño básico de la máquina en 1929, cuyo uso se generalizó prácticamente a la totalidad de los estamentos militares alemanes y la cúpula Nazi. En la marina alemana se la denominó con el nombre de máquina "M". Hasta la llegada al poder de Adolf Hitler en 1933 se habían fabricado en el mundo más de 100.000 unidades, llegando a ser utilizadas en países como Suecia, Holanda, Japón, Italia, España, EE.UU o Reino Unido entre otros.

La tercera máquina de cifrado de rotores fue desarrollada por el inventor holandés Hugo Alexander Koch. Dicha invención fue patentada el 7 de octubre de 1919 en Holanda. En vista del escaso éxito comercial que tuvo Koch (parece ser que no vendió ninguno de sus dispositivos de cifrado), éste le vendió algunos de los derechos de su máquina a Scherbius en 1927, por un valor de 600 florines holandeses. Algunos consideran que Scherbius le compró estos derechos a Koch con el fin de proteger su propia invención, ya que el alemán conocía a Koch ya que ambos habían colaborado estrechamente cuando Scherbius estaba desarrollando la Enigma.

La invención de la última máquina de cifrado de rotores se le atribuye al sueco Arvid Gerhard Damm, que la patentó tan sólo tres días después que Koch, el 10 de octubre de 1919. Su invención utilizaba un rotor doble cuya cadencia era irregular. En 1920, Damm fundó la empresa *Aktiebolaget Cryptograph* con el fin de comercializar su invención, sin embargo, se trataban de máquinas tremendamente erráticas, lo que hizo que Damm no pudiera tener el éxito comercial esperado, ya que sólo vendió unas pocas unidades. Dos de sus inversores eran Karl Wilhelm Hagelin y Emanuel Nobel (sobrino de Alfred Nobel). El hijo de Hagelin, Boris, que se habíua graduado en ingeniería mecánica en el Instituto Tecnológico de Estocolmo en 1919, se unió a la empresa en 1922 con el fin de proteger la inversión realizada. El ejército sueco encargó un gran pedido en 1926, sin embargo Damm no pudo disfrutar de su relativo éxito ya que moriría un año después. Un año antes, Boris Hagelin había tomado el control de la empresa (rebautizándola después con el nombre de *Aktiebolaget Cryptoteknik* en 1932), desarrollando de forma exitosa máquinas de cifrado con capacidad de imprimir (B-211) y una máquina totalmente portable (C-35). Un posterior diseño de Hagelin, la C-38, fue adquirida por el gobierno estadounidense y modificada bajo el permiso del propio Hagelin, siendo rebautizada como la M-209. Se vendieron más de 140.000 unidades de dicho modelo durante la 2ª Guerra Mundial, convirtiendo a Hagelin en el primero y posiblemente único millonario de este tipo de tecnología de máquinas de cifrado.

[3] http://ciphermachines.com/types.html

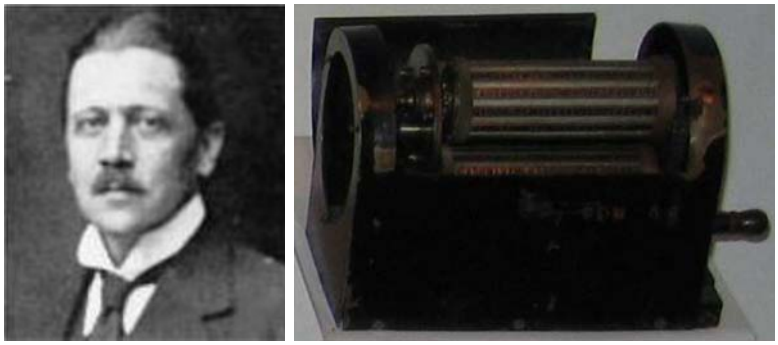

FIG. 3. ARVID GERHARD DAMM (izq.) y Prototipo Damm (drcha.).[3]

En el año 2003, se descubrió que la máquina de cifrado de rotores fue realmente inventada antes de los cuatro protagonistas mencionados anteriormente. Parece ser que en 1915, dos oficiales navales holandeses, THEO A. VAN HENGEL y R. P. C. SPENGLER, tuvieron la idea de construir un dispositivo de estas características mientras residían en las colonias holandesas del Este. Construyeron un prototipo en el verano de 1915, pero la armada holandesa no consideró que fuera una invención necesaria como para adoptarla en sus comunicaciones, además de disuadir a HENGEL y SPENGLER que intentaron patentar el dispositivo. Casualidades de la vida, uno de los abogados que inició el proceso de dicha patente era HUYBRECHT VERHAGEN, hermanastro de HUGO ALEXANDER KOCH. Esta coincidencia filial permitió con mucha probabilidad conocer dicha invención a KOCH, dándole la idea definitiva para desarrollar su dispositivo de cifrado.

1.2. El funcionamiento de Enigma. Enigma era muy similar a una máquina de escribir, salvo por que se alimentaba de una batería y no empleaba papel. Sus mensajes codificados se transmitían en código morse para ser descifrados por otra máquina Enigma al otro extremo de la línea. La máquina estaba formada por varias partes; un teclado de 26 caracteres, un clavijero interno o panel Stecker[4] con 6 pares de conexiones cableadas que podían conmutarse[5], un panel luminoso con 26 caracteres, varios rotores o modificadores (dependiendo de la versión de la Enigma), cada uno de los cuales contenía 26 muescas perimetrales con las 26 letras de alfabeto, y el reflector que devolvía el impulso eléctrico hacia los rotores una vez la señal había sido codificada. Cuando el operador pulsaba una tecla, enviaba un impulso eléctrico que recorría el interior de la máquina. Dicho impulso pasaba por el clavijero, donde era redirigido hasta el cilindro de entrada al conjunto de rotores que contenían el alfabeto. En estos

[4] Abreviatura de *Steckerverbindungen* que en alemán significa conexiones de clavija.

[5] Este número aumentó hasta 10 pares en sucesivas modificaciones con el fin de aumentar la seguridad de la máquina.

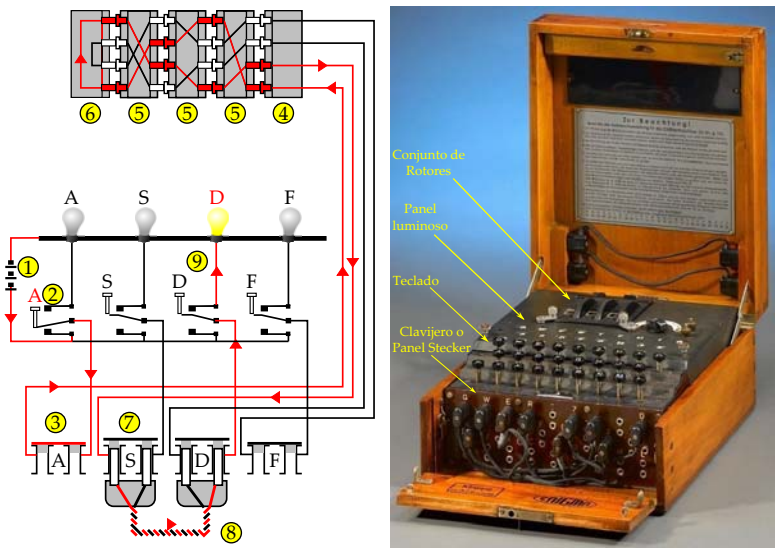

FIG. 4. Diagrama de funcionamiento de Enigma y partes de la misma.[6]

rotores era donde el operador llevaba a cabo los ajustes de la máquina. Unas ventanillas mostraban las letras en los rotores. Cada vez que el operador pulsaba una tecla, avanzaba una letra el rotor derecho o rápido. Una vez el rotor rápido diera toda una vuelta entonces giraba una posición el rotor central, es decir avanzaba una letra, y del mismo modo lo hacía el de la izquierda o lento con respecto al rotor central. El impulso eléctrico pasaba de derecha a izquierda a través de los cables de cada rotor, y era devuelto por un reflector de izquierda a derecha. En su viaje de vuelta el impulso pasaba por el clavijero nuevamente, y su destino final era el tablero luminoso, donde se iluminaba la letra transpuesta. La letra que se iluminaba se encendía dependiendo de los ajustes de la máquina, y esto se podía hacer en la cantidad de 150 millones de millones de millones de modos. El mensaje codificado era transmitido en código morse para ser descodificado por una máquina Enigma receptora ajustada en la misma clave diaria. En tiempos de guerra, estos ajustes se llegaron a realizar hasta tres veces al día.

[6] El diagrama representa el recorrido del impulso eléctrico desde que, una vez ajustada la configuración de los rotores (5), el operador pulsa la tecla A en el teclado (2), entonces el impulso eléctrico generado pasa por el clavijero o panel Stecker (3), de ahí pasa al cilindro de entrada (4), y entonces pasa por los rotores (5), y el reflector (6) que envía dicho impulso nuevamente a los rotores (5), cilindro de entrada (4), hasta que llega nuevamente al Stecker donde el impulso se direcciona con la conexión correspondiente (7 y 8), hasta que finalmente aparece iluminada la tecla codificada D (9) del tablero luminoso. Fuente: http://en.wikipedia.org/wiki/Enigma_machine

Sin duda el gran número de permutaciones posibles que la máquina era capaz de barajar, hicieron de ella que fuera considerada prácticamente inviolable. Éste fue uno de los motivos por el que pasó a formar parte del equipamiento de la armada alemana, no sin antes realizar varios cambios significativos como la introducción de un mayor número de rotores, con el fin de aumentar el número de posibilidades de cifrado. Este cambio la haría prácticamente inexpugnable a los ataques criptográficos, sin embargo, la historia probaría que los nazis estaban totalmente equivocados.

1.3. La operatividad de Enigma. El parámetro de configuración fundamental para operar con Enigma era la clave que tanto emisor como receptor debían conocer. Dicha clave estaba compuesta por:

- ✓ El orden de los rotores en los huecos de la máquina (*Walzenlage*).
- ✓ La posición inicial de éstos, que se configuraba colocando con la ruleta de la A a la Z (*Grundstellung*).
- ✓ Las conexiones del clavijero o panel Stecker.

Aunque no influía en la configuración de la clave, la distribución inicial de los anillos de los rotores (*Ringstellung*), que servía para variar la estructura del cableado interno de los mismos, también era un factor que podía modificarse.

Cada mes, los operadores de Enigma recibían un libro del alto mando con las claves diarias a utilizar en dicho mes[7], de modo que un operador podía leer en el libro algo así como:

- II-III-I.
- Y-B-J.
- A/G, F/H, J/L, M/O, R/T, U/X.

La configuración anterior le indicaba al operador que debía poner el segundo rotor en el hueco 1 y girarlo hasta la posición Y, el tercer rotor en el hueco 2 y girarlo hasta la B y el primer rotor en el hueco 3 y girarlo hasta la posición J. Así mismo debía conectar los cables en el panel Stecker con los pares de letras indicados. Una vez configurada la máquina, el operador podía comenzar a cifrar los mensajes que eran enviados mediante código morse. El receptor debía asimismo colocar la máquina en la misma disposición según el libro de códigos, y aquí es donde juega su papel el reflector. Simplemente tecletaría el mensaje cifrado recibido, y el mensaje original aparecería en el panel luminoso.

[7] A medida que avanzó la guerra, el número de claves pasó a ser de hasta tres diarias.

[8] De izq. a drcha. y de arriba a abajo: 1. Rotores de la Enigma. La parte posterior del rotor izqdo. muestra una muesca en la letra H (cada rotor tenía la suya) causante del giro de una posición del siguiente rotor situado inmediatamente a la izquierda. Por ejemplo los rotores I, II y III, tenían estas muescas en las letras Y, M y D, que provocaban el giro del rotor situado inmediatamente a su izquierda en las letras Q, E y V respectivamente. Inclusive la Kriegsmarine introduciría dos nuevos rotores (el IV y el V) que tenían doble muesca (en realidad los rotores de la anterior imagen son de este tipo), y causaban un aumento del número de giros de los mismos. 2. Disposición del anillo que se podía modificar para cambiar

Fig. 5. Rotores de Enigma.[8]

Los alemanes se dieron cuenta que operando de este modo, generaban un sinfín de mensajes con la misma clave durante todo un día (ya adelantaban que en periodos de operaciones bélicas, el tráfico de comunicaciones iba a ser inmenso), y esto resultaba un filón para los criptoanalistas. Conscientes de ello, emitieron una serie de órdenes sobre cómo se debía utilizar Enigma. De lo que no fueron conscientes es que al señalar una serie de normas estrictas, aunque al principio pudieran parecer sensatas, estaban proporcionando pistas para los criptoanalistas que significaron el principio del ataque a Enigma. Dichas normas eran fundamentalmente:

1. No se podía conectar una letra con su inmediatamente anterior o posterior en el panel Stecker.
2. Un rotor no podía permanecer en el mismo hueco durante más de un día.

Sin embargo la norma más importante resultó ser el concepto de "clave de mensaje". Con el fin de evitar un intenso tráfico de mensajes cifrados con la misma clave, lo que en sí mismo constituiría un filón para los criptoanalistas, los alemanes consideraron que cada mensaje enviado debía tener su propia clave. Pero, ¿cómo sabría el receptor la clave que había utilizado el emisor? Para ello el emisor configuraba la Enigma con la clave del día según el libro de códigos. Con dicha configuración, escribía tres letras elegidas al azar, por ejemplo FKM, obteniendo en el panel luminoso ZBH. Después, giraba los rotores desde su posición inicial (la indicada para ese día por el libro) a la posición de esas tres letras, en este caso F-K-M, dejando el orden de rotores y el panel Stecker sin

la configuración del cableado interno y la muesca del rotor. 3. Cableado interno de un rotor (diferente en cada rotor). 4. Reflector. 5. Interior del reflector. 6. Clavija interna del reflector modificable. http://www.cryptomuseum.com/crypto/enigma/m4/index.htm y http://naukas.com/2012/12/24/.

cambios, y entonces procedía a codificar el mensaje a enviar. De este modo el mensaje transmitido comenzaba ZBH, que era la codificación de FKM según la clave del día y el mensaje codificado según la disposición F-K-M de los rotores. El receptor, que tenía la máquina configurada con la clave del día, recibía la transmisión, y se fijaba en las primeras tres letras. Las tecleaba (ZBH en el ejemplo) y veía FKM. Entonces giraba los rotores a esa disposición, F-K-M, y tecleaba el resto del mensaje, obteniendo el original. Este hecho era característico de la Enigma como consecuencia de la propiedad recíproca que veremos más adelante.

Pero con el fin de evitar errores por interferencias en la transmisión o de los operadores, los alemanes obligaban a teclear dos veces seguidas las tres letras de la clave de mensaje. Así que realmente el emisor, con la clave del día, tecleaba FKMFKM, obteniendo en el panel luminoso ZBHGJI, y luego orientaba los rotores en la posición F-K-M y codificaba el mensaje. El receptor recibía el mensaje, tecleaba las seis primeras letras, ZBHGJI, y veía FKMFKM, con lo que ya reconocía la clave de mensaje. Sin embargo lejos de reforzar la seguridad de Enigma, esta norma ofreció a los criptoanalistas un punto de partida para comenzar a romper el código. Enigma, incumplía algunos de los principios de Kerckhoffs.

Principios de Kerckhoffs

En 1883, el lingüista y criptógrafo holandés Auguste Kerckhoffs (1835-1903) enunció en sus ensayos sobre criptografía militar los seis principios fundamentales que debían cumplirse para diseñar cualquier sistema criptográfico eficiente. Sus trabajos, más que una revisión del estado del arte de esta disciplina, significaron una auténtica renovación para las técnicas criptográficas del momento. Básicamente estos principios eran:

- ✓ Si el sistema no es teóricamente irrompible, al menos debe serlo en la práctica.
- ✓ La efectividad del sistema no debe depender de que su diseño permanezca en secreto.
- ✓ La clave debe ser fácilmente memorizable de manera que no haya que recurrir a notas escritas.
- ✓ Los criptogramas deberán dar resultados alfanuméricos.
- ✓ El sistema debe ser operable por una única persona.
- ✓ El sistema debe ser fácil de utilizar.

.

2. El origen del ataque a Enigma. El BS4.

2.1. 1ª Etapa. De Poznań a Varsovia. Tras la 1ª Guerra Mundial, los aliados se encargaron de vigilar las comunicaciones germanas. Sin embargo a

partir de 1926, comenzaron a interceptar mensajes cifrados mediante un nuevo método que desconocían hasta el momento. En medio de este desconcierto se encontraba el recientemente formado estado soberano de Polonia, el cual tenía al este a la Unión Soviética, un estado hambriento por expansionar su doctrina comunista fuera de sus fronteras, y al oeste Alemania, un estado que ansiaba recuperar los territorios cedidos a Polonia tras la guerra. En este clima de desconfianza, los polacos crearon su Oficina de Cifras, el *Biuro Szyfrów*, a mediados de 1931, surgido de la unión de la Oficina de Radio-Inteligencia (*Referat Radiowywiadu*) y la Oficina Criptográfica Polaca (*Referat Szyfrów Wlasnych*), e integrada en la 2ª Sección del ejército polaco, siendo su máximo responsable el teniente coronel Karol Gwido Langer, y el mayor Maksymilian Ciężki el jefe de la sección encargada de desencriptar los mensajes cifrados alemanes. Ciężki conocía la Enigma comercial, sin embargo, no tenía acceso a la Enigma militar, claramente distinta debido a los cambios introducidos en ella, por lo que al desconocer su cableado interno, fue incapaz de iniciar un ataque efectivo a su cifrado.

En enero de 1929, el director de la Universidad de Poznań (actualmente Universidad Adam Mickiewicz) Zdzislaw Krygowski preparó una lista de 20 estudiantes de matemáticas de últimos cursos que recibieron un llamamiento del ejército para participar en un curso de criptología. Bajo el juramento por parte de estos alumnos de mantener toda la operación en secreto, el curso se impartiría durante dos noches a la semana en dicha Universidad por el ya nombrado mayor Maksymilian Ciężki, Antoni Palluth, un ingeniero empleado civil del *Biuro Szyfrów*, y el mayor Franciszek Pokorny, por entonces jefe del mismo, emparentado con el famoso criptólogo del ejército austríaco durante la 1ª Guerra Mundial, el capitán Herman Pokorny. El curso tenía como principal propósito servir de apoyo al Servicio de Inteligencia Polaco de Radio con el fin de descifrar los mensajes alemanes interceptados. La razón de la elección de la Universidad de Poznań fue fundamentalmente debido a que la región de Pomerania, situada al oeste de Polonia, formó parte de la Prusia oriental, desde 1793 hasta 1918, por lo que sus habitantes hablaban perfectamente el alemán, de hecho a finales del siglo XIX, la escuela era obligatoriamente impartida en lengua germana. La otra razón de esta elección fue que, aunque no era demasiado conocido, la universidad contaba con un Instituto de Matemáticas.

Tras varias semanas, los estudiantes que asistieron a dicho curso fueron puestos a prueba para descifrar varios mensajes alemanes reales anteriores al uso de la Enigma que ya habían sido descifrados previamente. Con el fin de acotar su vocabulario se les daba una idea sobre el tema que trataba cada mensaje. Tras un par de horas, algunos estudiantes entre los que se encontraban Marian Rejewski, Jerzy Różycki y Henryk Zygalski, fueron capaces de descifrar los mensajes. A medida que el curso avanzaba, estos mensajes se fueron complicando paulatinamente, de modo que muchos estudiantes fueron abandonando

[9] http://fotopolska.eu/foto/13/13964.jpg

Fig. 6. Universidad de Poznań (1929).[9]

el curso bien porque preferían dedicarse enteramente a sus estudios, o bien porque consideraban que no tenían suficientes habilidades para la criptología. Únicamente los tres estudiantes antes nombrados fueron capaces de compaginar sus estudios con el curso. Uno de los exámenes a los que fueron sometidos era una comunicación militar alemana entonces actual cifrada mediante el código denominado "Cifrado de Doble Transposición". Los tres estudiantes, cada uno de manera independiente, fueron capaces de romper dicho código, poniendo de manifiesto que estaban dotados de ciertas habilidades criptológicas. Muy a su pesar, Rejewski tuvo que abandonar el curso antes de su finalización, puesto que recibió una beca para estudiar en la Universidad de Gotinga, sueño de cualquier estudiante de matemáticas, puesto que allí habían impartido clases eminencias como Gauss, Riemann, Dirichlet, Poincaré o Hilbert entre otros.

En el verano de 1930, Rejewski regresó a Poznań. Al finalizar el curso, los mejores estudiantes del mismo fueron invitados para colaborar con el Biuro Szyfrów cuyas oficinas estaban en los sótanos de la comandancia militar polaca equipadas con todo lo necesario para descifrar los mensajes alemanes. De forma general se permitía a los estudiantes compaginar sus tareas criptológicas con sus estudios, de manera que su trabajo en el Biuro Szyfrów se distribuía generalmente en doce horas semanales en el turno que ellos prefirieran, ya fuera diurno o incluso nocturno. La "cámara oscura" (como llamaban los estudiantes a los oficinas del Biuro) estaba en el puesto de la comandancia militar, tan sólo a unos pasos del Instituto de Matemáticas para que los estudiantes no tuvieran que perder demasiado tiempo en el trayecto y aprovechar así sus tiempos muertos. Rejewski comenzó a trabajar allí en el otoño de 1930.

Método de Doble Transposición

Se trata de un código utilizado por el ejército de los EE.UU en la 1ª Guerra Mundial, prácticamente idéntico al código UBCHI alemán. Consiste fundamentalmente en realizar una primera transposición del texto plano según las letras de una o dos claves, así por ejemplo, la palabra clave ENIGMA, equivaldría a la clave 264351 (los números representan el orden de las letras de la palabra clave en el alfabeto). Se coloca el texto plano en una matriz de tantas columnas como letras posea la palabra clave, escribiendo por filas, y se realiza una primera transposición por columnas. Una vez hecha esta operación se vuelven a coger las columnas transpuestas y se escriben nuevamente por filas, y se realiza la segunda transposición por columnas, en este paso se podría hacer uso de una segunda palabra clave. Veamos como se cifraría el mensaje "REPLEGAR TROPAS EN TORNO A LA POSICION INICIAL", con la única palabra clave ENIGMA.

1 2 3 4 5 6		2 6 4 3 5 1		1 2 3 4 5 6		2 6 4 3 5 1
R E P L E G		E G L P E R		E R S N O N		R N N S O E
A R T R O P		R P R T O A		A G P O A I		G I O P A A
A S E N T O		S O N E T A		C L R N A I		L I N R A C
R N O A L A	⇒	N A A O L R	⇒	N P T E O S	⇒	P S E T O N
P O S I C I		O I I S C P		I L E O T L		L L O E T I
O N I N I C		N C N I I O		C I R A A R		I R A R A C
I A L		A L I		P O I		O I P

Finalmente se agrupaban en grupos de cinco letras para su transmisión posterior en código Morse, resultando:

RGLPL IONII SLRNO PRTER IOAAO TAEAC NICP

Se formó de este modo un grupo de trabajo de jóvenes matemáticos, cuya principal tarea consistía en el descifrado de todo tipo de códigos alemanes. Los estudiantes recibían constantemente información de varias estaciones de radio dedicadas a interceptar mensajes cifrados de los alemanes quienes regularmente cambiaban sus claves, y rápidamente aprendieron incluso a aprovechar los errores cometidos por los operadores alemanes, como por ejemplo el hecho de que necesitaran mensajes de al menos 50 caracteres de longitud. Los estudiantes descubrieron que los alemanes caracterizaban estos mensajes más cortos con la letra "X" y a continuación codificaban el mismo. Sin embargo, a pesar de sus más que notables habilidades criptológicas, aparecieron unos cifrados que no podían romper independientemente de las técnicas utilizadas. El uso de la

Enigma se había instaurado de forma total en el ejército alemán y era el momento de "profesionalizar" las tareas criptológicas de los estudiantes polacos. En el verano de 1932, el puesto de Poznań fue cerrado y Rejewski primero, y Różycki y Zygalski un poco después, comenzaron a trabajar como empleados del Biuro Szyfrów en Varsovia. Nacía así el BS4 y comenzaba la guerra contra Enigma.

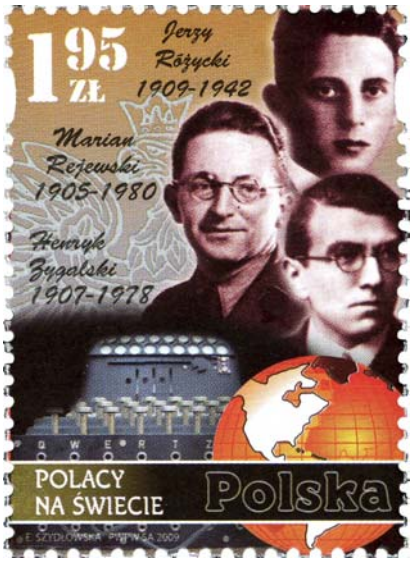

Fig. 7. Miembros del BS4.[10]

2.2. 2ª Etapa. La aparición de *Asché*. El trabajo del BS4 se basó fundamentalmente en el estudio de la repetición de patrones. El patrón más obvio de la encriptación de la Enigma era la clave de mensaje, que se codificada dos veces al principio de cada mensaje. Los alemanes habían exigido dicha repetición para prevenir posibles errores causados por las intermitencias de radio o fallos del operador, sin embargo no previeron que esto pondría en peligro la seguridad de la máquina. A pesar de que los polacos del BS4 realizarían un gran avance en el descubrimiento del funcionamiento de Enigma mediante el análisis de los patrones de repetición, consiguiendo identificar que las cadenas de caracteres cifrados tenían una relación dependiente exclusivamente de la posición de los rotores de la máquina, al principio su principal limitación era su desconocimiento sobre la distribución del cableado interior de la máquina, ya que no contaban con ninguna máquina física del ejército alemán. Este hecho añadido a que los alemanes modificaban el cableado interior de las máquinas

[10] Sello polaco (2009). http://www.wnsstamps.ch/en/stamps/PL039.09

que adquirían con el fin de evitar posibles espionajes que comprometieran la integridad de sus comunicaciones, impidieron en primera instancia que los polacos del BS4, del que formaba parte el joven REJEWSKI entre otros, fueran capaces de descifrar los mensajes interceptados.

Existe un punto de vista erróneo que se repite sistemáticamente en multitud de publicaciones, y que no es otro que considerar que la ruptura del código de Enigma se produjo de una manera puntual, cosa que no fue así puesto que los polacos llevaron a cabo pequeños logros que se tradujeron finalmente en comprender el funcionamiento de la Enigma y consecuentemente establecer una estrategia eficaz para desentrañar el código de encriptación que la máquina escondía. El primer intento de búsqueda de la desencriptación del código Enigma llevaría en torno a cuatro meses, proceso que debía considerar dos cuestiones bien diferenciadas:

1. Por un lado la reconstrucción teórica de la Enigma militar. Los criptólogos polacos descubrirían primero la función del reflector (Umkehrwalze), tras lo cual reconstruyeron poco a poco todas conexiones existentes en la máquina, cuyos principales componentes eran el sistema de rotores (Chiffrierwalzen) que giraban sobre un eje común, y el panel de conexiones o clavijero (Steckerverbindungen). Esto supuso que los polacos fueran capaces de construir una réplicas de la Enigma que hacían posible la lectura de los mensajes cifrados alemanes una vez se encontraran las claves de configuración de los rotores.
2. Por otro lado estaba el proceso de elaboración de los métodos para la reconstrucción de las claves de la Enigma basándose únicamente en los mensajes interceptados por las estaciones polacas de radiomonitoreo.

Es en este momento en el que hace su aparición la figura de HANS THILO SCHMIDT, un corrupto y resentido funcionario de la *Chiffrierstelle* en Berlín, la oficina responsable de administrar las comunicaciones cifradas de Alemania. SCHMIDT, que sirvió en la 1ª Guerra Mundial y fue expulsado del ejército después de los recortes producidos en el mismo tras la firma del armisticio en Versalles, había entrado en la oficina de cifras a través de la intervención de su hermano RUDOLF, un reputado oficial alemán con una trayectoria en ascenso al que parece ser que se le atribuye la idea de sugerir al alto mando del ejército alemán que se considerara la Enigma con el objetivo de salvaguardar la seguridad de las comunicaciones. SCHMIDT tenía fama de mujeriego y parece que le gustaba vivir por encima de las posibilidades que un puesto como el suyo le podía proporcionar. Fue entonces cuando a través de la embajada de Francia en Berlín, accedió a intercambiar información valiosa sobre el funcionamiento de Enigma a cambio de cuantiosas prebendas. Así fue como el servicio secreto francés, a través de la intermediación del entonces capitán GUSTAV BERTRAND y el agente secreto cuyo pseudónimo era *Rex*, obtuvo copia de varios documentos sobre el funcionamiento de Enigma de manos de SCHMIDT el 8 de noviembre de

1931 en el Grand Hotel de Verviers, Bélgica. Se establecieron varias reuniones entre septiembre y octubre de 1932, en las que SCHMIDT, cuyo nombre en clave era *Asché* (pronunciación francesa de *H*), proporcionó los libros de códigos con todas las claves del día completas para 38 meses firmados por el teniente coronel ERICH FELLGIEBEL (más tarde nombrado general y jefe de la sección de comunicaciones de la Wehrmacht), así como fotos de la máquina, aunque en ningún caso ninguna documentación sobre el cableado interno de los rotores. Sin embargo, muy a su pesar, los criptoanalistas franceses fueron incapaces de sacar partido a dicha información. Por ello, en virtud del tratado de colaboración que franceses y polacos habían firmado tras la 1ª Guerra Mundial, y dado que el Biuro Szyfrów estaba muy interesado en todos los asuntos relacionados con Enigma, la inteligencia francesa decidió compartir esta información con sus homónimos polacos, lo que significó un punto de inflexión en el ataque al código de Enigma. SCHMIDT trabajó en la *Chiffrierstelle* hasta 1938. El 23 de marzo de 1943 sería arrestado y supuestamente reconoció su espionaje en julio de ese año. Finalmente se suicidaría el 19 de septiembre de 1943.

FIG. 8. H. T. SCHMIDT y K. G. LANGER.[11]

El jefe del Biuro Szyfrów, GWIDO LANGER, tomó una desconcertante pero astuta decisión. No entregó en primera instancia los libros de claves a REJEWSKI hasta finales de 1932, consciente de que éstas no estarían disponibles en tiempos de guerra. De este modo obligó al propio REJEWSKI a entrenar sus capacidades criptoanalíticas en tiempo de paz en previsión del inminente conflicto bélico que inevitablemente estaba a punto de estallar. En este punto, REJEWSKI y sus colegas no tuvieron más remedio que agudizar su ingenio para buscar una manera de romper el código de la Enigma. REJEWSKI que contaba con alguna Enigma comercial buscó refugio en las matemáticas puras

[11] http://pippick.com/reviews/worldfaceoff/worldtimer_faceoff.htm y http://enigma.umww.pl/index.php?page=gwido-langer

y abstractas, en particular en el estudio de las permutaciones dentro de la rama denominada como teoría de grupos. Uno de los pilares fundamentales para el análisis criptológico en general son el estudio de las repeticiones, en el caso de Enigma, Rejewski comenzó por estudiar los únicos patrones de repetición que conocía, la clave de los mensajes que se repetía al inicio de cada uno de ellos.

2.3. El Método de las Permutaciones. Fundamentación Teórica.

2.3.1. Teoría de Permutaciones. Introducción. El grupo de las permutaciones de S, siendo $S = \{x_1, x_2, \ldots, x_n\}$ un conjunto finito de n elementos, resulta ser el ejemplo de grupo finito más utilizado en la rama matemática denominada *teoría de grupos*. En 1854, Arthur Cayley demostró que todo grupo es isomorfo a un subgrupo de un grupo simétrico, y si el grupo es finito y tiene orden n, entonces es isomorfo a un subgrupo de S, resultado que pone de manifiesto el poder de unificación característico de la teoría de grupos, al ser capaz de condensar en un único grupo abstracto, todos los grupos provenientes de las distintas áreas de las matemáticas. Por ejemplo, el nacimiento de la teoría de grupos permitió asociar a cada polinomio un grupo de permutaciones de sus raíces, lo que posibilitó establecer los criterios fundamentales para la solubilidad por radicales de dicho polinomio, resultado que se conoce como *teoría de Galois*.

Denominada originalmente *Teoría de Sustituciones*, históricamente fueron muchos los matemáticos que se dedicaron a su estudio, como Euler, Lagrange, Ruffini, Abel, Gauss, Galois, Cayley o Sylow entre otros.

Si X es un conjunto no vacío, una *permutación* de X es una biyección $\alpha : X \to X$. Denotamos el conjunto de todas las permutaciones de X por S_X.

Si θ es una *permutación* de S, podemos representarla mediante una matriz de correspondencias de la forma

$$\theta = \begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ x_{i1} & x_{i2} & \ldots & x_{in} \end{pmatrix}$$

donde $\theta\, x_1 = x_{i1}$, $\theta\, x_2 = x_{i2}$, $\ldots$, $\theta\, x_n = x_{in}$, es decir el elemento x_1 se convierte en el x_{i1}, $\ldots$. De este modo, una permutación del conjunto S puede ser representada sin ambigüedad por una permutación del conjunto $\{1, 2, \ldots, n\}$. El conjunto de estas permutaciones se denota por S_n y se denomina *Grupo simétrico de grado n*. Se demuestra que para $n \geq 3$, S_n no es abeliano. La correspondencia descrita es claramente una aplicación biyectiva, ya que podemos encontrar una aplicación inversa θ^{-1} de modo que su composición genera la aplicación identidad ($\theta \circ \theta^{-1} = I$). Veamos un ejemplo:

$$\theta = \begin{pmatrix} a & b & c & d & e & f \\ c & a & b & d & e & f \end{pmatrix};$$

$$\theta^{-1} = \begin{pmatrix} c & a & b & d & e & f \\ a & b & c & d & e & f \end{pmatrix} = \begin{pmatrix} a & b & c & d & e & f \\ b & c & a & d & e & f \end{pmatrix}$$

Cuando se tienen dos permutaciones σ y θ en S_n, el producto $\sigma\,\theta$ se interpreta como composición de aplicaciones, es decir $\sigma\,\theta\,(m) = \sigma\,(\theta(m))$, para todo $m \in \{1, 2, \ldots, n\}$. Es fácilmente demostrable ver que dicha operación en general no es conmutativa, es decir $\sigma\,\theta \neq \theta\,\sigma$. Veamos un ejemplo:

$$\sigma = \begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix};\ \ \theta = \begin{pmatrix} a & b & c & d \\ d & c & b & a \end{pmatrix}$$

$$\sigma\theta = \begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix} \cdot \begin{pmatrix} a & b & c & d \\ d & c & b & a \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ a & d & c & b \end{pmatrix}$$

$$\theta\sigma = \begin{pmatrix} a & b & c & d \\ d & c & b & a \end{pmatrix} \cdot \begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ c & b & a & d \end{pmatrix}$$

El conjunto de elementos $\{1, 2, \ldots, n\}$ que son movidos por una permutación θ, se denota A_θ y se denomina el *soporte de la permutación.*

Dos permutaciones σ y θ se dicen que son *disjuntas*, si $A_\sigma \cap A_\theta = \varnothing$. Veamos un ejemplo:

$$\theta = \begin{pmatrix} a & b & c & d & e & f \\ b & c & a & d & e & f \end{pmatrix};\ \ \sigma = \begin{pmatrix} a & b & c & d & e & f \\ a & b & c & e & f & d \end{pmatrix} \Rightarrow$$

$\Rightarrow A_\theta = \{a, b, c\}$ y $A_\sigma = \{d, e, f\}$, claramente σ y θ son disjuntas.

Teorema.- *Si σ y θ son permutaciones disjuntas en S_n, entonces conmutan, es decir $\sigma\,\theta = \theta\,\sigma$.*

Una permutación $\theta \in S_n$ se denomina *ciclo*, si existen elementos $s_1, s_2, \ldots, s_k$ en el conjunto $\{1, 2, \ldots, n\}$ tales que:

1. Se tienen las relaciones $\theta(s_1) = s_2$, $\theta(s_2) = s_3$, $\ldots$, $\theta(s_{k-1}) = s_k$, y $\theta(s_k) = s_1$.
2. La permutación θ deja fijos a todos los elementos de $\{1, 2, \ldots, n\}$ distintos de los s_i.

Con la finalidad de expresar la permutación anterior, se utiliza la notación cíclica $\theta = (s_1, s_2, \ldots, s_k)$. Al entero k se le denomina *orden* o *longitud del ciclo.*

Teorema.- *Toda permutación es o bien un ciclo, o se puede descomponer como un producto de ciclos disjuntos. Esta descomposición o factorización es única salvo por el orden de los factores.*

Sea $\sigma = \sigma_1\sigma_2 \cdots \sigma_t$ un producto de ciclos disjuntos de longitudes respectivas $m_1, m_2, \ldots, m_t$. El orden de la permutación σ es el $m.c.m(m_1, m_2, \ldots, m_t)$.

Sea $\sigma = (i_1, i_2, \ldots, i_m)$ un ciclo de longitud m. Entonces $\sigma^{-1} = (i_m, \ldots, i_2, i_1)$ también es un ciclo de longitud m.

Sea $\sigma = \sigma_1\sigma_2 \cdots \sigma_t$ un producto de ciclos disjuntos de longitudes respectivas $m_1, m_2, \ldots, m_t$. Entonces $\sigma^{-1} = \sigma_1^{-1}\sigma_2^{-1} \cdots \sigma_t^{-1}$.

Un ciclo de longitud 2 se denomina *transposición.*

Teorema.- *Toda permutación se puede descomponer como un producto de transposiciones. Dicha descomposición no es única.*

Teorema.- *Sea la permutación $\theta \in S_n$. Entonces θ no puede ser descompuesta como un producto de un número par e impar de transposiciones simultáneamente.*

Dos permutaciones σ y θ en S_n se consideran *conjugadas*, si existe otra permutación $\varphi \in S_n$ tal que

$$\theta = \varphi\sigma\varphi^{-1}$$

Sea σ una permutación cuya descomposición en producto de ciclos disjuntos tiene m_1 ciclos de longitud 1, m_2 ciclos de longitud 2, y en general m_k ciclos de longitud k, se denomina *tipo* o *estructura de ciclos* de la permutación σ al producto formal $1^{m_1}2^{m_2}\cdots k^{m_k}$.

Teorema.- *Dos permutaciones son conjugadas si y sólo sí son del mismo tipo.*

2.3.2. La estrategia de Rejewski. A pesar de que la tesis de Marian Rejewski titulada *Teoría de funciones periódicas dobles de segunda y tercera especie y sus aplicaciones*, estaba más cerca del análisis que del álgebra, estaba muy familiarizado con la teoría de grupos, y conocía bastante bien las permutaciones. Desde un punto de vista formal, una permutación puede considerarse como una reordenación de elementos. Por ejemplo cuando ordenamos las lista de nuestros alumnos por orden alfabético de sus apellidos, o cuando barajamos un mazo de cartas, estamos realizando un cambio del orden de estos conjuntos que puede ser representado mediante una permutación.

Imaginemos por un instante que tenemos un conjunto de seis elementos: “a”, “b”, “c”, “d”, “e”, y “f”[12]. Una permutación podría ser la siguiente:

- ✓ “a” se convierte en “c”, (“a” → “c”)
- ✓ “b” se convierte en “a”, (“b” → “a”)
- ✓ “c” se convierte en “b”, (“c” → “b”)
- ✓ “d” se convierte en “f”, (“d” → “f”)
- ✓ “e” se convierte en “d”, (“e” → “d”)
- ✓ “f” se convierte en “e”, (“f” → “e”)

De esta manera, la permutación que denominaremos P, transforma el conjunto ordenado (abcdef) en el conjunto ordenado (cabfde). Una manera de indicar la permutación es haciendo cadenas cíclicas, esto es, por un lado “a” → “c”, “c” → “b”, “b” → “a”, y por otro “d” → “f”, “f” → “e”, “e” → “d”, de forma que tenemos dos ciclos cerrados de tres elementos cada uno de ellos. Podremos por lo tanto expresar la permutación P como:

$$\mathrm{P} = (\mathrm{acb})(\mathrm{dfe})$$

[12] Con la intención de seguir un esquema de exposición formal, notaremos en mayúsculas a las permutaciones y en minúsculas las letras del alfabeto.

Rejewski supo vislumbrar la conexión entre la matemática abstracta y teórica con el mecanismo de funcionamiento de la máquina Enigma a través de las permutaciones, esperando que la teoría de grupos fuera capaz de extraer alguna propiedad sencillamente asociable a la configuración de los rotores, reduciendo en gran medida el enorme número de posibilidades combinatorias de rotores, reflector y clavijero.

La Enigma era una máquina construida para llevar a cabo permutaciones de letras. Si el operario pulsaba una tecla, la señal eléctrica pasaba a través de diferentes elementos de la máquina, representando cada uno de ellos una permutación (ver Fig. 4). Primero lo hacía por el clavijero, en el que algunas letras eran intercambiadas. La señal eléctrica seguía su camino hasta el cilindro de entrada que es como un rotor fijo, donde se producía una segunda permutación. A continuación, la señal eléctrica entraba en el sistema de rotores, primero en el derecho (o rápido), después en el central y por último en el izquierdo (o lento). Después la señal rebotaba en el reflector e iniciaba su camino de vuelta en orden inverso hasta encender la bombilla correspondiente a la letra cifrada. Desde un punto de vista meramente formal, podemos representar el camino de la señal eléctrica como el producto de las siguientes permutaciones:

- ✓ S: permutación causada por el clavijero o panel Stecker.
- ✓ H: permutación causada por el cilindro de entrada.
- ✓ N: permutación causada por el rotor derecho.
- ✓ M: permutación causada por el rotor central.
- ✓ L: permutación causada por el rotor izquierdo.
- ✓ R: permutación causada por el reflector.

De la misma manera, la señal eléctrica en su camino de vuelta, volvía a sufrir nuevas permutaciones, de forma que si por ejemplo el rotor lento (o izquierdo) provocaba una permutación L cuando la señal iba de derecha a izquierda hasta llegar al reflector, dicho rotor introduciría una permutación inversa a L, que denominaremos L^{-1}, en el camino de vuelta de dicha señal. Del mismo modo, ocurre con el resto de elementos, teniéndo así las permutaciones M^{-1}, N^{-1}, H^{-1}, S^{-1}, que resultan ser las permutaciones inversas de M, N, H y S respectivamente. Si llamamos I al camino de ida de la señal eléctrica, y V al camino de vuelta de la misma, podremos expresar se recorrido tal y como representa la tabla anexa.

Por lo tanto, el efecto neto de pulsar una tecla viene representado por la permutación compuesta $SHNMLRL^{-1}M^{-1}N^{-1}H^{-1}S^{-1}$, o lo que es lo mismo, $(SHNML)\,R\,(SHNML)^{-1}$, es decir cualquier permutación de Enigma se traduce en una permutación conjugada del reflector.

El reflector era un "medio rotor". Tenía únicamente 26 contactos en su lado derecho. Internamente, los 26 contactos estaban conectados con cables por parejas, de tal manera que la permutación resultante del reflector consistía en 13 transposiciones disjuntas.

Sentido	Elemento que atraviesa	Permutación Total
I	Clavijero	S
I	Cilindro de entrada	SH
I	Rotor drcho.	SHN
I	Rotor central	SHNM
I	Rotor izq.	SHNML
	Reflector	SHNMLR
V	Rotor izq.	$SHNMLRL^{-1}$
V	Rotor central	$SHNMLRL^{-1}M^{-1}$
V	Rotor drcho.	$SHNMLRL^{-1}M^{-1}N^{-1}$
V	Cilindro de entrada	$SHNMLRL^{-1}M^{-1}N^{-1}H^{-1}$
V	Clavijero	$SHNMLRL^{-1}M^{-1}N^{-1}H^{-1}S^{-1}$

Los alemanes utilizaron el mismo tipo de reflector para todos los modelos de la Enigma, el cual era completamente desconocido para los polacos. La permutación provocada por el reflector era la siguiente:

$$R = (ae)(bj)(cm)(dz)(fl)(gy)(hx)(iv)(kw)(nr)(op)(pu)(st)$$

Por lo tanto, como la permutación global de Enigma debe ser del mismo tipo que la provocada por el reflector ya que son conjugadas (ver pág. 102), dicha permutación global puede descomponerse siempre en producto de 13 transposiciones disjuntas. Sin embargo, se ha de enfatizar el hecho de que cuando el operario pulsaba una tecla, el rotor derecho (o rápido) giraba, y únicamente tras el giro se cerraba el circuito eléctrico. Este hecho llevó a Rejewski a tomar en consideración una nueva permutación que transforma cualquier letra en la siguiente, es decir a $\to$ b, b $\to$ c, etc. Rejewski denominó a esta permutación P, y es igual a:

$$P = (abcdefghijklmnopqrstuvwxyz)$$

que utilizando la notación de ciclos representada anteriormente, significa que "a" se convierte en "b", "b" se convierte en "c", y así sucesivamente. Por lo tanto cuando el rotor derecho gira, se tiene que se aplica la permutación P, luego la N y después la inversa de P, es decir PNP^{-1}. Cuando la señal realiza el camino de vuelta, la permutación será justo la inversa, es decir $P^{-1}N^{-1}P$.

En segundo lugar, a medida que el operario pulsaba por segunda vez una tecla cualquiera, el rotor derecho giraba otra vez, sufriendo la señal entrante la permutación $PPNP^{-1}P^{-1}$, o lo que es lo mismo P^2NP^{-2}, y la saliente la inversa de ésta, es decir $P^{-2}N^{-1}P^2$.

También habrá que considerar que cada vez que finalice un ciclo completo el rotor derecho, el central girará una posición, y completado el rotor central su ciclo, entonces girará el rotor izquierdo una posición. Este hecho obliga a considerar dichos movimientos a la hora de formalizar la permutación global. Llegado a este punto, Rejewski se encargó de analizar las relaciones matemáticas de las seis primeras letras cifradas. Si imaginamos los rotores y el clavijero

en una disposición concreta, es muy probable que tras pulsar seis teclas, ni el rotor central ni el izquierdo giraran, ya que la probabilidad de que la pulsación de seis teclas hiciera girar el rotor central era de 6/26, mientras que la de que gire el izquierdo es aún muchísimo menor. Por lo tanto no es descabellado considerar esta hipótesis de partida.

Cualquiera que sea la tecla que se pulsara, la señal eléctrica que generaba daba lugar a la siguiente permutación, que denominaremos A:

$$\begin{aligned} \mathrm{A} &= \mathrm{SHPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}H^{-1}S^{-1}} = \\ &= (\mathrm{SHPNP^{-1}ML})\,\mathrm{R}\,(\mathrm{SHPNP^{-1}ML})^{-1} \end{aligned} \tag{1}$$

En una segunda pulsación, el nuevo movimiento del rotor derecho, provocaba que la permutación de A fuera alterada. Por lo tanto, la pulsación de una segunda tecla haría que la señal sufriera la permutación B:

$$\begin{aligned} \mathrm{B} &= \mathrm{SHP^{2}NP^{-2}MLRL^{-1}M^{-1}P^{2}N^{-1}P^{-2}H^{-1}S^{-1}} = \\ &= (\mathrm{SHP^{2}NP^{-2}ML})\,\mathrm{R}\,(\mathrm{SHP^{2}NP^{-2}ML})^{-1} \end{aligned} \tag{2}$$

Del mismo modo expresaríamos una tercera, cuarta, quinta y sexta pulsaciones, que llamaremos C, D, E y F respectivamente, resultando:

$$\begin{aligned} \mathrm{C} &= \mathrm{SHP^{3}NP^{-3}MLRL^{-1}M^{-1}P^{3}N^{-1}P^{-3}H^{-1}S^{-1}} = \\ &= (\mathrm{SHP^{3}NP^{-3}ML})\,\mathrm{R}\,(\mathrm{SHP^{3}NP^{-3}ML})^{-1} \end{aligned} \tag{3}$$

$$\begin{aligned} \mathrm{D} &= \mathrm{SHP^{4}NP^{-4}MLRL^{-1}M^{-1}P^{4}N^{-1}P^{-4}H^{-1}S^{-1}} = \\ &= (\mathrm{SHP^{4}NP^{-4}ML})\,\mathrm{R}\,(\mathrm{SHP^{4}NP^{-4}ML})^{-1} \end{aligned} \tag{4}$$

$$\begin{aligned} \mathrm{E} &= \mathrm{SHP^{5}NP^{-5}MLRL^{-1}M^{-1}P^{5}N^{-1}P^{-5}H^{-1}S^{-1}} = \\ &= (\mathrm{SHP^{5}NP^{-5}ML})\,\mathrm{R}\,(\mathrm{SHP^{5}NP^{-5}ML})^{-1} \end{aligned} \tag{5}$$

$$\begin{aligned} \mathrm{F} &= \mathrm{SHP^{6}NP^{-6}MLRL^{-1}M^{-1}P^{6}N^{-1}P^{-6}H^{-1}S^{-1}} = \\ &= (\mathrm{SHP^{6}NP^{-6}ML})\,\mathrm{R}\,(\mathrm{SHP^{6}NP^{-6}ML})^{-1} \end{aligned} \tag{6}$$

Para poder resolver el sistema de ecuaciones representado por las seis ecuaciones que equivalen a las seis pulsaciones de teclas en Enigma, Rejewski necesitaba conocer N, M, L y R, ya que de este modo podría averiguar la configuración del cableado de los rotores y el reflector. De manera adicional necesitaba conocer S y H, es decir, las permutaciones del clavijero y del cilindro de entrada, ya que estos eran desconocidos. Sin embargo lejos de resultar un sistema compatible determinado, Rejewski partía con el gran handicap de desconocer las permutaciones A, B, C, D, E y F. Para que éstas fueran conocidas, sería necesario conocer el texto llano junto con el cifrado, y las estaciones de radioescucha únicamente proporcionaban el segundo.

Aparentemente las investigaciones de Rejewski se situaban en un callejón sin salida, sin embargo, no estamos ante un personaje común, de ahí la genialidad de sus resultados. En conocimiento de la Enigma comercial, Rejewski basó sus investigaciones en tres resultados fundamentales a la hora de obtener la configuración interna del cableado de los rotores, esto es equivalente a determinar N, M, L y R.

El primer resultado proviene de una propiedad de la Máquina Enigma denominada *reciprocidad*, de tal forma que se puede demostrar que $A^{-1} = A$, $B^{-1} = B$, etc. Esto significa que para una configuración concreta de los diferentes elementos de la máquina Enigma, si pulsamos "s" y obtenemos "r", también podemos pulsar "r" y obtenemos "s".

El segundo resultado crucial consistió en aprovechar una de las debilidades ocasionadas por la repetición de las claves. En primer lugar el operador que iba a emitir un mensaje cifrado debía consultar el libro de claves con el fin de obtener la clave maestra (la que iban a utilizar todos los operadores ese día) que representaba la configuración inicial de partida de los rotores. Imaginemos que "sol" es dicha clave maestra. A continuación el operador elegía una "clave de sesión"[13] para cifrar el mensaje. Imaginemos que dicha clave es "oro". El proceso entonces era el siguiente:

1. El operador cifraba las letras "oro" con la clave "sol" (es decir, ponía los rotores de forma que en la ventana superior de la máquina apareciera "s-o-l"), obteniendo en el panel luminoso "buu".
2. Entonces el operador colocaba los rotores en la posición representada por las letras "o-r-o", y procedía a cifrar el mensaje.
3. El operador enviaba "buu" junto con el mensaje cifrado.

El operador que recibía el mensaje realizaba la operación inversa. Tomaba el libro de claves, colocaba su máquina con los rotores en la posición "s-o-l", tecleaba "buu" y obtenía en el panel luminoso la clave del mensaje "o-r-o". Una vez hecho eso, colocaba los rotores en la posición "o-r-o" y tecleaba el mensaje cifrado obteniendo en el panel luminoso el texto plano.

Sin embargo, debido a que los mensajes se transmitían, entre otros medios, por radio, existía la posibilidad de que se produjeran errores de transmisión ocasionados por perturbaciones atmosféricas, además de considerar que en ocasiones se producían errores de transcripción de los operadores. Con el fin de evitar estos posibles fallos, los alemanes establecieron la norma de que la clave del mensaje debía ser cifrada dos veces. Esto es, en el caso que hemos visto, la máquina se ponía en la posición "s-o-l", y se tecleaba "o-r-o-o-r-o", obteniéndose "buurqr". De este modo el receptor del mensaje cifrado recuperaría la clave del mensaje repetida, o de lo contrario, tendría así dos posibilidades para ensayar y obtener el mensaje descrifrado.

[13] También llamada clave del mensaje.

El hecho de repetir la clave del mensaje dos veces, significó encontrar un punto de partida para comenzar el ataque a Enigma. Las repeticiones son un filón para los criptoanalistas y Rejewski no dejó pasar inadvertida la sutil relación que existía en el cifrado de la clave del mensaje. Imaginemos que alguien interceptase el mensaje con la clave de mensaje cifrada "buurqr". Está claro que existe una relación entre las letras primera y cuarta, esto es "b" y "r". Nosotros sabemos que equivalen a la letra "o", pero el criptoanalista sabe que tras pulsar una tecla desconocida (llamémosla "x") obtiene "b", y que cuando pulsa en cuarta posición, obtiene "r". Haciendo uso del lenguaje de permutaciones explicado al principio de esta sección, la permutación A nos indica de qué manera cambian las letras cuando se pulsa una tecla por primera vez, y D lo mismo pero cuando se pulsa una letra por cuarta vez. Esto es equivalente a considerar:

$$\mathrm{A(x) = b;\ D(x) = r}$$

El criptoanalista desconoce "x", pero en virtud de la propiedad recíproca de Enigma, sabe que A(b) = x. Puesto que A transforma "b" en "x", y D transforma "x" en "r", la permutación compuesta AD (es decir, la que se obtiene de aplicar A, y después D) nos transforma "b" en "r":

$$\mathrm{AD(b) = r}$$

Por lo tanto el criptoanalista desconocía las permutaciones A y D, pero sí que conocía parte de la permutación AD, únicamente considerando el resultado de cifrar la clave del mensaje dos veces ("buurqr") y establecer la relación entre la primera letra y la cuarta. A lo largo del día se interceptaría una cantidad suficiente de mensajes para establecer más indicativos. Si consideramos los siguientes indicativos de un día dado:

1: (gtaasw)	2: (edjwmv)	3: (ngevjt)	4: (rdjdmv)
5: (cdjqmv)	6: (ntwvso)	7: (dldjbn)	8: (qlaxbw)
9: (zlapbw)	10 (udekmt)	11: (pgjejv)	12: (qtsxsx)

donde se puede ver las siguientes relaciones "g" → "a", "e" → "w", "n" → "v", "r" → "d", ... En general interceptando unos ochenta mensajes diarios, el criptoanalista podía construirse la siguiente tabla de relaciones:

1ª letra:	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
4ª letra:	i	r	q	j	w	c	a	y	o	z	f	b	t	v	u	e	x	d	g	h	k	s	m	n	l	p

obteniendo así la permutación completa AD, ordenada por la longitud de sus ciclos:

$$\mathrm{AD} = (\mathrm{aioukfcqxnvsg})(\mathrm{brdjzpewmthyl})^{14}$$

[14] Obsérvese que la permutación resultante se puede descomponer en un número par de ciclos de idéntica longitud cada pareja. Este hecho no pasó desapercibido para Rejewski, que lo denominó *característica*.

De igual forma, el criptoanalista podría realizar un análisis idéntico con la segunda y quinta letras de la clave del mensaje cifrado y con la tercera y la sexta, conociendo así las permutaciones compuestas BE y CF respectivamente. No olvide el lector que el fin último de todo este "engendro" es lograr conocer el cableado de los rotores y del reflector, o lo que es lo mismo conocer las permutaciones N, M, L y R.

Veamos cómo llevó a cabo Rejewski esta proeza matemática. Para llegar al fin último antes descrito, tuvo que probar innumerables combinaciones, propiedades, teoremas y leyes. En primer lugar, se construía, gracias a los mensajes interceptados, las permutaciones compuestas AD, BE y CF.

Rejewski centró su atención en el hecho de que la permutación S cambiaba únicamente seis pares de letras, mientras que las restantes catorce letras permanecían invariables. Con el fin de aligerar la notación matemática, denominaremos Q a la permutación producida por el reflector y los rotores central y derecho, es decir $Q = MLRL^{-1}M^{-1}$. De este modo las permutaciones resultan:

$$A = SHPNP^{-1}QPN^{-1}P^{-1}H^{-1}S^{-1}$$
$$B = SHP^{2}NP^{-2}QP^{2}N^{-1}P^{-2}H^{-1}S^{-1}$$
$$C = SHP^{3}NP^{-3}QP^{3}N^{-1}P^{-3}H^{-1}S^{-1}$$
$$D = SHP^{4}NP^{-4}QP^{4}N^{-1}P^{-4}H^{-1}S^{-1}$$
$$E = SHP^{5}NP^{-5}QP^{5}N^{-1}P^{-5}H^{-1}S^{-1}$$
$$F = SHP^{6}NP^{-6}QP^{6}N^{-1}P^{-6}H^{-1}S^{-1}$$
$$AD = SHPNP^{-1}QPN^{-1}P^{3}NP^{-4}QP^{4}N^{-1}P^{-4}H^{-1}S^{-1}$$
$$BE = SHP^{2}NP^{-2}QP^{2}N^{-1}P^{3}NP^{-5}QP^{5}N^{-1}P^{-5}H^{-1}S^{-1}$$
$$CF = SHP^{3}NP^{-3}QP^{3}N^{-1}P^{3}NP^{-6}QP^{6}N^{-1}P^{-6}H^{-1}S^{-1}$$

Con la representación anterior, Rejewski conocía las permutaciones compuestas AD, BE y CF, y desconocía las permutaciones H, S, N y Q. En un primer intento, consideró que H, es decir la permutación que representa el cilindro de entrada, debiera ser la misma para el modelo militar que para el modelo comercial. Aunque esta suposición resultó ser totalmente errónea, consideremos como punto de partida que la suponemos conocida.

El siguiente paso consistía en determinar A, B, C, D, E y F, considerando únicamente como punto de partida las permutaciones compuestas AD, BE y CF, para lo cual Rejewski utilizó varios teoremas.

Teorema. (Sobre el Producto de Transposiciones) *Si dos permutaciones del mismo tipo están factorizadas únicamente como producto de transposiciones disjuntas, entonces su producto contiene un número par de ciclos disjuntos de la misma longitud.*

Rejewski argumentó su demostración así:

$$\text{Si } X = (a_1\, a_2)\,(a_3\, a_4)\,(a_5\, a_6)\,\ldots\,(a_{2k-3}\, a_{2k-2})\,(a_{2k-1}\, a_{2k}),$$
$$\text{e } Y = (a_2\, a_3)\,(a_4\, a_5)\,(a_6\, a_7)\,\ldots\,(a_{2k-2}\, a_{2k-1})\,(a_{2k}\, a_1),$$
$$\text{entonces } XY = (a_1\, a_3\, a_5\,\ldots\,a_{2k-3}\, a_{2k-1})\,(a_{2k}\, a_{2k-2}\,\ldots\,a_6\, a_4\, a_2).$$

y continuaba [3, p. 262]:

> *"Si, de este modo, no hemos agotado todas las letras de la permutación, continuaremos nuestro procedimiento hasta que lo hayamos hecho."*

La composición de permutaciones es una actividad muy común en álgebra abstracta, pero lo que realmente necesitaba Rejewski era factorizar las permutaciones AD, BE y CF.

Teorema. (Opuesto al Teorema sobre el Producto de Transposiciones) *Si en cualquier permutación de grado par aparecen un número par de ciclos disjuntos de la misma longitud, entonces la permutación puede ser considerada como un producto de dos permutaciones consistentes en transposiciones disjuntas.*

Hay que poner de manifiesto que las permutaciones AD, BE y CF satisfacen las condiciones de este teorema. Su demostración es inmediata a partir de lo indicado anteriormente.

> Dada $XY = (a_1\, a_3\, a_5\, \ldots\, a_{2k-3}\, a_{2k-1})\,(a_{2k}\, a_{2k-2}\, a_5\, \ldots\, a_6\, a_4\, a_2)$,
> entonces podemos expresar:
> $X = (a_1\, a_2)\,(a_3\, a_4)\,(a_5\, a_6)\,\ldots\,(a_{2k-3}\, a_{2k-2})\,(a_{2k-1}\, a_{2k})$,
> e $Y = (a_2\, a_3)\,(a_4\, a_5)\,(a_6\, a_7)\,\ldots\,(a_{2k-2}\, a_{2k-1})\,(a_{2k}\, a_1)$

Teorema. *Los elementos que forman parte de una única transposición, bien sea de la permutación X, o bien sea de la permutación Y, forman parte siempre de dos ciclos distintos de la permutación compuesta XY.*

Teorema. *Si dos elementos que se encuentran en dos ciclos diferentes de igual longitud de la permutación XY, pertenecen a la misma transposición, entonces las letras adyacentes a ellas (una por la derecha y la otra por la izquierda) también pertenecen a la misma transposición.*

Teorema. (Sobre las Permutaciones Conjugadas) *Si K(i) = j; esto es, K = (... ij ...); entonces $T^{-1}KT$ = (... T(i) T(j) ...). Nótese que esto implica que K = (... ij ...) y $T^{-1}KT$ = (... T(i) T(j) ...) tiene idéntica descomposición en ciclos disjuntos.*

Para la demostración, Rejewski consideró que $T\,(T^{-1}KT)\,(i) = KT\,(i) = T(K(i)) = T(j)$. En particular, esto significa que la introducción de las permutaciones puede ser ordenada de forma que

$$K = (\ldots\ldots\, i\ j\, \ldots\ldots)$$

$$T^{-1}KT = (\ \ldots\ T(i)\ T(j)\ \ldots)$$

que describe la permutación T.

Con respecto a las permutaciones A, B y C, se podían obtener unas cuantas soluciones (hasta una docena), de las cuales sólo una era la correcta. En este punto, no se podría saber a priori cuál debiera ser la solución correcta. Sin

embargo, en ocasiones se interceptaban mensajes transmitidos por operarios no demasiado "cuidadosos" que habían cifrado dichos comunicados con claves de mensaje relativamente sencillas del tipo "j-j-j", "z-z-z", u otras como "q-w-e", "b-n-m" que indicaban teclas dispuestas consecutivamente en el teclado de la Enigma. Este hecho podía resultar un punto de apoyo para poder determinar cuál de las soluciones para A, B, y C era la correcta.

En este punto del proceso criptoanalítico, Rejewski no conocía aún siquiera si las ecuaciones que dan A, B, C, D, E, y F resultaban ser despejables para obtener S, N y Q. Podían resolverse en el caso de que el criptoanalista tuviera a su disposición los mensajes de dos días diferentes (en los cuales las conexiones del clavijero fueran diferentes pero los rotores estuvieran en las mismas posiciones), pero el enorme número de distintas posiciones y orientaciones de los rotores hacían de este un problema inviable en la práctica.

Es aquí cuando Rejewski se apoyo en los documentos proporcionados por el espía alemán Hans Thilo Schmidt, que llegaron a sus manos de manera inesperada el 9 de diciembre de 1932. Además de las permutaciones AD, BE, CF (obtenidas mediante radioescucha) y las A, B, C, D, E y F (deducidas por los criptoanalistas polacos), ahora se conocía también la permutación S, y dejaba de ser por lo tanto una incógnita, y consecuentemente resultaba despejable, junto con H (recuerde el lector que hemos partido de la hipótesis de que H es conocida, aunque después se demuestre que no es cierto), resultando:

$$\begin{aligned}
H^{-1}S^{-1}ASH &= PNP^{-1}QPN^{-1}P^{-1}\\
H^{-1}S^{-1}BSH &= P^2NP^{-2}QP^2N^{-1}P^{-2}\\
H^{-1}S^{-1}CSH &= P^3NP^{-3}QP^3N^{-1}P^{-3}\\
H^{-1}S^{-1}DSH &= P^4NP^{-4}QP^4N^{-1}P^{-4}\\
H^{-1}S^{-1}ESH &= P^5NP^{-5}QP^5N^{-1}P^{-5}\\
H^{-1}S^{-1}FSH &= P^6NP^{-6}QP^6N^{-1}P^{-6}
\end{aligned}$$

donde únicamente se tienen las incógnitas N y Q. Rejewski definió las permutaciones U, V, W, X, Y y Z del siguiente modo:

$$\begin{aligned}
U &= P^{-1}H^{-1}S^{-1}ASHP = NP^{-1}QPN^{-1}\\
V &= P^{-1}H^{-1}S^{-1}BSHP = NP^{-2}QP^2N^{-1}\\
W &= P^{-1}H^{-1}S^{-1}CSHP = NP^{-3}QP^3N^{-1}\\
X &= P^{-1}H^{-1}S^{-1}DSHP = NP^{-4}QP^4N^{-1}\\
Y &= P^{-1}H^{-1}S^{-1}ESHP = NP^{-5}QP^5N^{-1}\\
Z &= P^{-1}H^{-1}S^{-1}FSHP = NP^{-6}QP^6N^{-1}
\end{aligned}$$

A continuación, Rejewski calculó las permutaciones compuestas UV, VW, WX, XY e YZ, resultando:

$$\begin{aligned}
UV &= NP^{-1}[QP^{-1}QP]PN^{-1}\\
VW &= NP^{-2}[QP^{-1}QP]P^2N^{-1}\\
WX &= NP^{-3}[QP^{-1}QP]P^3N^{-1}\\
XY &= NP^{-4}[QP^{-1}QP]P^4N^{-1}
\end{aligned}$$

$$YZ = NP^{-5}[QP^{-1}QP]P^5N^{-1}$$

Despejó el factor $[QP^{-1}QP]$ de una de las anteriores ecuaciones y lo introdujo en las otras cuatro, obteniendo:

$$VW = NP^{-1}N^{-1}UVNPN^{-1}$$
$$WX = NP^{-1}N^{-1}VWNPN^{-1}$$
$$XY = NP^{-1}N^{-1}WXNPN^{-1}$$
$$YZ = NP^{-1}N^{-1}XYNPN^{-1}$$

donde la única incógnita resulta ser la permutación NPN^{-1}. En un día normal, se puede estimar que había del orden de varias decenas de soluciones para VW, WX, XY e YZ, pero lo más importante de todo ello es que estas permutaciones mantenían una estructura común. De no ser así, esto únicamente podía significar dos cosas, bien que se había cometido un error ese día, o bien que ese día en particular el movimiento del rotor lento (situado más a la izquierda) inducía movimiento en el rotor medio para alguna de las posiciones, por lo que era necesario en este caso volver a empezar con otro día. Utilizando el mismo método empleado para obtener A, B, C, D, E y F partiendo de AB, CD, y EF, puede determinarse NPN^{-1} partiendo de XW, obteniendo varias posibles soluciones. También se pueden obtener distintas soluciones a partir de la ecuación WX, y únicamente existe solución idéntica para las ecuaciones VW y WX. De igual forma, se puede obtener N a partir de NPN^{-1}, para lo cual bastaba aplicar una cualquiera de las 26 posibles permutaciones P que existen para obtener la N, que resultaba ser la permutación inducida por el cableado del rotor que estaba en la posición lenta de ese día.

Sin embargo el lector no debe olvidar que Rejewski supuso erróneamente una hipótesis que luego resultó ser falsa. Consideró que la permutación H era la misma que la de la Enigma comercial: los cables iban de las teclas al cilindro de entrada en el orden del teclado qwert ... Sin embargo, al probarlo con la Enigma militar, el método no funcionaba. La permutación H era otra. De hecho, los alemanes podían haber incluido en H cualquier permutación que les hubiese dado la gana, y el número de permutaciones distintas con 26 elementos es inmensa. Pero Rejewski logró dar con la clave de este problema a finales de 1932 o principios de 1933, considerando que los alemanes, tan ordenados y metódicos, tal vez hubieran considerado H como la permutación alfabética. Es decir, las teclas se unirían mediante cables al cilindro de entrada siguiendo un orden abcdef ... Rejewski probó dicha hipótesis, experimentando a buen seguro un sentimiento de triunfo al observar que resultaba ser correcta. De hecho, se comenta que cuando en verano de 1939 los polacos compartieron sus descubrimientos con sus aliados, la primera pregunta de Dillwyn Knox a Rejewski fue *"¿cuál era la permutación del cilindro de entrada?"*. Al oír la respuesta tan trivial, parece que Knox montó en cólera por no haber pensado en tan obvia posibilidad.

2.4. 3ª Etapa. La amenaza de la invasión y la búsqueda de aliados. Rejewski repitió el mismo proceso con las relaciones que existían entre los caracteres 2º y 5º, y los 3º y 6º de la clave de los mensajes. En este punto, llegó a la conclusión que estas cadenas de caracteres eran una consecuencia directa de la configuración y disposición de los rotores y que el clavijero influía únicamente en que las letras cambiaban, es decir variaban las permutaciones, pero la estructura cíclica de éstas permanecía invariable aún cuando la configuración del clavijero cambiara. Por lo tanto el número de ciclos y sus longitudes dependía única y exclusivamente del orden en el que estaban dispuestos los rotores y de su configuración inicial de partida. Rejewski denominó *característica* a este número de ciclos y longitudes. El número de características que los polacos tenían que estudiar se reducía por lo tanto drásticamente de 10^{16} a 105.456, o lo que es lo mismo $6 \times 26 \times 26 \times 26$, que siendo aún un número grande, sí que permitía abordar manualmente el ataque al código de Enigma. Con respecto a las *características*, Rejewski comentaba [11, p. 217]:

> *"Esta estructura es la más característica, y aunque su representación difiere cada día, su rasgo es siempre el mismo: en cada línea los ciclos de idéntica longitud aparecen siempre por parejas. Observando el papel que dicha estructura jugaba, la denominé estructura característica, o simplemente la característica de un día determinado."*

Rejewski pasó algo más de un año recopilando lo que denominó *catálogo de características*, y gracias a sus descubrimientos, los polacos fueron capaces de construir un catálogo para cada configuración de rotores. Con la ayuda del libro de claves proporcionado por Schmidt, se pudo llevar a cabo con éxito la tarea de desencriptación. Schmidt había proporcionado los libros con las claves de septiembre y octubre (es decir de dos trimestres diferentes), lo que permitió deducir la configuración de dos rotores. Bastaba esperar hasta el comienzo del año 1933, para que los polacos pudieran obtener la configuración del tercer rotor y deducir así la del reflector. A últimos de enero de 1933, el código de la Enigma había sido descubierto.

Tras el incendio del Reichstag a últimos de febrero de 1933, y con la subida al poder de lo que después se convertiría en el régimen nazi, los polacos del BS4, a petición de Rejewski, consideraron oportuno reforzar las tareas criptológicas, por lo que la plantilla se aumentó a 6 operarios de descifrado, entre ellos

[15] El Palacio Sajón sirvió de cuartel general de la comandancia polaca, donde en 1932 los polacos consiguieron romper el código Enigma por primera vez. En la imagen se puede ver la estatua ecuestre del Príncipe Józef Poniatowski. La galería contiene la Tumba del Soldado Desconocido en memoria a los soldados polacos caídos en combate durante la 1ª Guerra Mundial (1914-1918) y la guerra con la Unión Soviética (1918-1920). Durante la 2ª Guerra Mundial gran parte del edificio y alrededores (la Plaza Jósef Pilsudski o el Palacio Brühl) fueron totalmente destruidos. http://www.herder-institut.de/warschau/ausschnitt_04/ausschnitt-04_01.html

Fig. 9. Palacio Sajón en Varsovia (entre 1930 y 1935).[15]

Jerzy Różycki y Henry Zygalski, los cuales habían sido minuciosamente entrenados con anterioridad.

Con el fin de mecanizar la tarea de encontrar el catálogo adecuado para una configuración determinada, los polacos construyeron unas réplicas de la Enigma militar. Antoni Palluth, Edward Fockczyński, y los hermanos Ludomir y Leonard Danilewicz, ingenieros y directores de la compañia de Radiomanufactura AVA, encargada de surtir al Biuro Szyfrów todo tipo de material tecnológico para comunicaciones, acometieron la fabricación de dichas réplicas de Enigma que se construyeron casi artesanalmente durante la noche para mantener el asunto en completo secreto. Un operario de total confianza llevaba a cabo el ensamblaje mecánico de dicha máquina. AVA que había sido fundada en 1929 y tenía sus oficinas centrales en el número 34 de la calle Nowy Swiat en Varsovia, recibió el encargo de la comandancia general polaca para llevar a cabo la construcción de 15 de estas réplicas a principios de febrero de 1933, y concluyó la entrega de dicho encargo a mediados de 1934.

Durante los primeros meses de la primera victoria polaca sobre Enigma, los operarios tenían que obtener la configuración inicial de manera prácticamente manual, de forma que giraban los rotores metálicos con 17.576 posibilidades, habiendo 263 posibles configuraciones. Esta tarea resultaba, además de tediosa, profundamente dolorosa puesto que los dedos de los criptólogos llegaban a sangrar, ya que no era posible que éstos delegaran dicha actividad en el personal técnico. Fue entonces cuando Rejewski, con ayuda de Antoni Palluth, inventó el "ciclómetro", un mecanismo que permitió manejar a los criptólogos polacos un catálogo de 105.456 características. El ciclómetro era una máquina

Enigma doble (con seis ruedas y dos reflectores) pero en la que el segundo juego de ruedas se ajustaba automáticamente tres posiciones con respecto al primero. El efecto que se conseguía es el mismo que si se pulsase una tecla en una máquina convencional, es decir, se teclean otras dos y luego se teclea la misma otra vez, únicamente que con el ciclómetro sólo era necesario teclear una vez, en lugar de cuatro. Durante tres años las comunicaciones encriptadas con Enigma resultaron ser un libro abierto para los polacos. Sin embargo, para su desgracia, el 1 de noviembre de 1937, los alemanes cambiaron el reflector de las máquinas, lo que significó tener que reconstruir nuevamente el catálogo.

En enero de 1938, la comandancia general polaca llevó a cabo una investigación interna con el fin de cuantificar la eficacia del trabajo del BS4. Los resultados del estudio realizado durante dos semanas fueron bastante concluyentes, ya que ponían de manifiesto que el equipo formado por diez individuos (entre criptólogos y operadores) era capaz de descifrar alrededor del 75 % de todos los mensajes interceptados, lo que daba una idea del éxito de los polacos, considerando que parte de los mensajes interceptados resultaban en ocasiones ilegibles o incompletos debido a las interferencias.

El 27 de Mayo de 1938, los polacos invitaron a Gustave Bertrand, el comandante de la inteligencia francesa que ya les había proporcionado los documentos de H. T. Schmidt, para que éste conociera el nuevo centro en Pyry, en los bosques de Kabackie, unos diez kilómetros al sur de Varsovia, cuyo nombre en clave era "Wicher" (Vendaval), donde además le mostrarían los logros conseguidos por el BS4.

Para desdicha de los polacos, el 15 de septiembre de 1938 los alemanes volvieron a dar una vuelta de tuerca con el fin de buscar la optimización de la Enigma. Esta vez los cambios introducidos dejaron inservibles por completo todos los métodos de desencriptación llevados a cabo hasta el momento. Dichos cambios consistían básicamente en que tanto la configuración de los rotores, como las claves eran elegidas libremente por el operador en cuestión. Las tres letras de la clave se transmitían de forma abierta en la cabecera del mensaje y éstas precedían a las seis letras que resultaban del doble cifrado de la clave del mensaje. Por ejemplo, la cabecera "FDA GHRMER" indicaba que la configuración de los rotores era FDA (con el orden de los rotores establecido previamente en los libros por el alto mando nazi, y que en aquel momento cambiaba todos los días), y las otras seis letras correspondían al cifrado doble de la clave del mensaje. Todo el resto del proceso no sufrió ningún cambio significativo adicional, aunque cabe destacar que por entonces, el número de conexiones del Stecker estaba entre cinco y ocho.

Los cambios introducidos se traducían en una modificación de la configuración de los rotores en cada uno de los mensajes, lo cual a su vez provocaba la modificación de los productos AD, BE y CF, sin embargo, los alemanes continuaban cometiendo el mismo error, que consistía en repetir la clave del mensaje

al inicio de cada comunicación. Los polacos aprovecharon esta pequeña debilidad. Con el fin de elaborar el catálogo de características, calcularon 105.456 productos posibles de AD. Pudieron comprobar que el 40 % de estas permutaciones contenían ciclos de longitud 1, y del mismo modo ocurría con los productos BE y CF. Pongamos un ejemplo, supongamos que tenemos tres mensajes interceptados con las siguientes cabeceras:

FDE BWHBXT QSC GJVBJM ZDR WSXTGX

Como podemos observar subrayado se produce la repetición en idénticas posiciones de algunos caracteres. Los británicos acuñarían el término *female* para referirse a dichas repeticiones. El mensaje con la cabecera FDE BWHBXT, indica que la permutación AD correspondiente contiene el ciclo (B). Utilizando la terminología introducida por los británicos, dicha cabecera se expresaba como una 1,4-female. Del mismo modo, en el segundo mensaje con la cabecera QSC GJVBJM, tendríamos una 2,5-female y (J) es un ciclo de la permutación BE, y en el tercer mensaje con la cabecera ZDR WSXTGX tendríamos una 3,6-female y (X) es un ciclo de CF.

Recordemos que las conexiones del Stecker no tenían ninguna influencia en las longitudes de las permutaciones AD, BE y CF, ya que dichas longitudes dependían única y directamente del orden de los rotores y de sus posiciones iniciales, viniendo determinadas por las diferencias entre las letras del Grundstellung y las del Ringstellung (ver 1.3). Por un lado, el Grundstellung era distinto en cada uno de los mensajes, aunque conocido, sin embargo, el Ringstellung era el mismo en todos los mensajes de un mismo día, aunque desconocido. El objetivo fundamental del trabajo criptológico consistía fundamentalmente en identificar correctamente el orden de cada uno de los rotores y la configuración del anillo de entre las 105.456 posibles configuraciones. Sorprendentemente, este enorme número de posibilidades se reducía en un factor de 0,4 cada vez que aparecía un ciclo de longitud 1, ya que únicamente el 40 % de las permutaciones AD (o bien las BE, o las CF) presentaban este tipo de ciclos unitarios. Si las permutaciones AD, BE y CF eran elegidas de manera aleatoria, la teoría de probabilidades arrojaba un resultado sorprendente, y es que el 11,5 % de las cabeceras de los mensajes presentaban females. De este modo, se necesitaban únicamente doce o trece females entre un centenar de mensajes interceptados para determinar de manera unívoca el orden de los rotores y el Ringstellung.

De forma adicional al trabajo desarrollado por Rejewski, en septiembre de 1938 Zygalski inventó un ingenioso método que proporcionaría a los polacos la posibilidad de descifrar de manera masiva los mensajes cifrados interceptados, ya que determinaba el orden de los rotores y el Ringstellung. El método de las *hojas de Zygalski* o *Netz* (del alemán *Netzverfahren*, "método neto"), rudimentario aunque bastante efectivo, basaba su fundamentación en la aparición de females. Zygalski preparó 6 paquetes de 26 hojas cada uno, donde cada paquete representaba una posible configuración de los rotores (cada uno de los 6

órdenes posibles de los rotores y cada una de las 26 posiciones del rotor izquierdo). En cada una de las hojas se escribía una letra y a continuación se dibujaba una cuadrícula de 51×51 (60×60 cms aprox.) en la que se rotulaban tanto las abscisas como las ordenadas con todas las letras, comenzando por la esquina superior izquierda. Las letras horizontales representan las posiciones del rotor central y las verticales las del derecho, de modo que cada pequeño cuadrado, representaba una permutación con ciclos de una letra correspondiente a esa posición de los rotores, es decir una female. Los cuadrados correspondientes a las 1,4-females se perforaban directamente. Sin embargo las 2,5 y 3,6-females, necesitaban un proceso de "normalización" que consistía básicamente en adelantar su Grundstellung derecho una o dos posiciones respectivamente. Utilizando el ejemplo presentado en la página 115:

QSC GJVBJM ⇒ QTC GJVBJM ZDR WSXTGX ⇒ ZDT WSXTGX

Realizada la nombrada normalización, se procedía a repetir el proceso para cada orden de los rotores y cada posición del Ringstellung del rotor izquierdo. Fijado el orden de los rotores, se normalizaban de nuevo aquellas females cuyo Grundstellung se tradujera en un avance del rotor central. Pongamos un ejemplo, imaginemos que el orden de los rotores era II-I-III, y que el Grundstellung era SGV. Dicho Grundstellung debía ser normalizado a SHV, ya que la V es la letra que provoca en el rotor III un avance del rotor situado inmediatamente a su izquierda, en este caso el rotor central en el que se encuentra el I. Acto seguido, se seleccionaban el juego de 26 hojas asociadas al orden de rotores establecido, y fijada una letra del Ringstellung del rotor izquierdo, pongamos por ejemplo la letra F, se consideraba el Grundstellung de una primera female. Supongamos que una 1,4-female era RDW. Como R-F=M, se escogía la hoja correspondiente a la letra M que servía de patrón básico con el que comenzar a trabajar, y se colocaba sobre una mesa transparente iluminada por debajo. A continuación se tomaba otra 1,4-female, pongamos por ejemplo MYS. Como M-F=H, se seleccionaba la hoja correspondiente a H y se colocaba sobre el patrón básico representado por la letra M, pero desplazada 5 pequeños recuadros hacia la derecha (ya que de la Y a la D van 5 letras), y 4 pequeños recuadros hacia abajo (porque de la S a la W van 4 letras). Se repetía la operación con el resto de females, y una vez colocadas todas las hojas se observaba si la luz de la iluminación que había debajo de la mesa transparente traspasaba algún agujero común a todas ellas. Si se habían conseguido una cantidad suficiente de females, el haz de luz atravesaba un único agujero, el cual proporcionaba de manera inmediata el orden de los rotores y el Ringstellung del rotor izquierdo. Con el fin de obtener el de los otros dos rotores, es necesario observar que, fijada una de las females (normalizada si ha sido necesario), las letras del agujero de la hoja correspondiente determinaban la posición de los rotores que la había producido. Dicha posición era precisamente la diferencia entre el Grundstellung de la female y el Ringstellung que se pretendía obtener. Por consiguiente, el Ringstellung de los rotores central y derecho se obtení restando al Grundstellung de

una female las letras del agujero. Como última operación quedaba obtener las conexiones del Stecker. Recordemos que el Stecker no cambiaba la estructura de ciclos, sino que únicamente alteraba las letras de los mismos, en este caso los de longitud 1 del catálogo de características por las letras repetidas de las females, entonces la letra repetida de una female estaba conectaba con una de las letras de los ciclos de longitud 1 de la correspondiente permutación AD del catálogo. Contemplando todas las females a un tiempo, no era difícil averiguar cual.

Pero, ¿qué ocurría si el haz de luz atravesaba más de un agujero? En ese caso se procedía a realizar las anteriores operaciones con cada uno de ellos, y las contradicciones descartaban casi todos los casos, permitiendo considerar la solución correcta como aquella que permitía descifrar los mensajes.

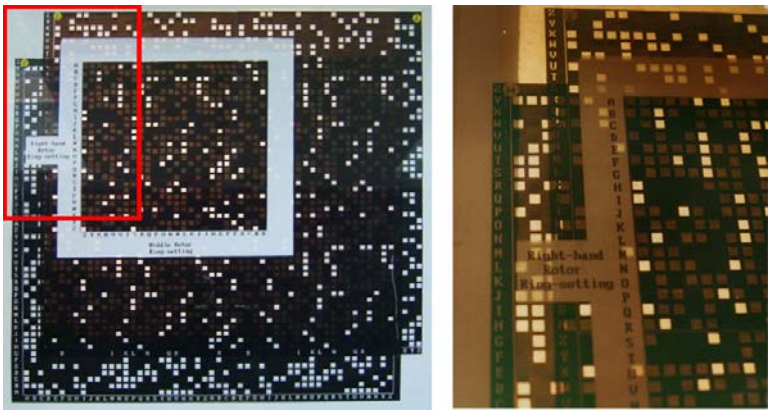

FIG. 10. Hojas de Zygalski en el Museo de Bletchley Park.[16]

Por otro lado, también JERZY RÒŻYCKI contribuyó en gran medida a la lucha contra Enigma desarrollando el denominado *método del reloj*, que hacía posible determinar en ocasiones cuál de los rotores estaba en la posición del rotor derecho o rápido. Su método fue más tarde perfeccionado en Bletchley Park por Alan Turing, desarrollando la técnica denominada *bamburismo*. Hasta finales de 1935, los alemanes cambiaban el orden de los rotores sólo una vez cada tres meses, por lo que hasta entonces obtener la disposición del rotor rápido no resultaba de tan vital importancia. Sin embargo, a partir del 1 de febrero de 1936, dicho cambio se empezó hacer cada mes, y el 1 de noviembre de ese año comenzó a hacerse cada día, de ahí la importancia de obtener la disposición del rotor rápido. Veamos un ejemplo para ver en qué consistía dicho ingenioso método. Imaginemos que tenemos dos textos en alemán y los ponemos uno debajo del otro letra a letra como muestra la siguiente tabla.

[16] http://en.wikipedia.org/wiki/Zygalski_sheets

W E M G O T T W I L L R E C H T E G U N S T ...
D E R A L T E L A N D M A N N A N S E I N E N ...

Se puede observar que de media existirá una probabilidad de coincidencia de letras en ambos textos de 2/23. Debemos esperar que esta característica se repita con textos cifrados mediante una clave idéntica. Sin embargo si se encripta cada texto utilizando una clave distinta (en este caso se utilizaron las claves O-G-P y J-N-C, con las conexiones E/G, J/Y, S/O, en el Stecker) resultan los mensajes cifrados que se muestran en la siguiente tabla.

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

La tabla anterior muestra que en este caso, la probabilidad de que coincidan letras en la misma posición en los dos textos cifrados con claves diferentes es de 1/23. Este hecho se debe a la distinta frecuencia de aparición de las letras en idioma alemán. En un lapso de 23 letras este hecho no ocurrirá demasiadas veces. Si por el contrario se tuvieran dos mensajes de 260 letras de longitud, con este método se podría generalmente diferenciar si los dos mensajes se cifraron con idéntica clave o con diferentes. Para ello teniendo disponible una cantidad suficiente de material cifrado, normalmente se podía encontrar una docena de pares de mensajes tales que en cada pareja las primeras dos letras de las claves eran idénticas, mientras que las terceras letras eran diferentes. Entonces, se escribían ambos mensajes uno encima de otro. Existían dos posibles formas de escribir un mensaje encima de otro, dependiendo de en qué posición de partida se encontrara el rotor rápido una vez que se producía el desplazamiento del rotor medio. Estas posiciones eran conocidas y diferentes para cada uno de los tres rotores. Por ejemplo, si el rotor I estaba colocado en la posición del rotor rápido, entonces el desplazamiento del rotor medio ocurría cuando el rotor rápido se desplazaba de la letra Q a la R. Si el rotor II estaba situado en la posición del rotor rápido, el desplazamiento sucedía cuando se desplazaba de la letra E a la F, y si el rotor III se situaba en la posición del rotor rápido, el desplazamiento sucedía cuando se desplazaba de la V a la W. Para cada una de las dos formas de escribir los mensajes, era suficiente contar el número de columnas con idénticas letras para determinar cuál era el modo correcto de escribir los mensajes y por lo tanto determinar cuál de los tres rotores estaba localizado en la posición del rotor rápido. De todos los métodos criptológicos desarrollados por el BS4, el método del reloj era el único que tomaba en consideración las características propias del lenguaje alemán, esto es, la frecuencia de aparición de las letras de su alfabeto.

La lucha constante entre la optimización de los recursos polacos y los cambios sucesivos realizados en la Enigma militar por parte de los alemanes, significó desarrollar no una única técnica, sino varios métodos que permitieran desentrañar el código de Enigma de la mejor manera posible. Además de las

hojas de Zygalski o el método del reloj de Różycki, hubo otros como el *método ANX*. Los polacos utilizaron un hecho bastante llamativo, y es que el texto en claro de muchos mensajes alemanes interceptados comenzaban por "ANX" ("AN" significa PARA en alemán y la "X" se empleaba como separador de palabras). Una vez que era determinada la posición inicial del rotor derecho en un mensaje que comenzara por "ANX", la de los otros dos rotores se podía obtener mediante la utilización del catálogo de características construido por Rejewski.

Tras los últimos cambios en los reflectores, los alemanes buscaban la utilización óptima de la Enigma, sin embargo continuaban cometiendo el mismo error, que consistía en repetir la clave del mensaje al inicio de cada comunicación. Con la ayuda de unas invenciones basadas en las réplicas de Enigma, Rejewski fue capaz de encontrar la clave del día de las comunicaciones alemanas antes de que acabara el día. Dichas invenciones, denominadas *bombas*, resultaron ser unos aparatos electro-mecánicos basados en la combinación de 6 réplicas de la Enigma polaca construida previamente, y tenían como principal objetivo mecanizar su sistema de catalogación de modo que pudieran encontrar las posiciones correctas de los rotores. La máquina era capaz de probar 17.576 combinaciones diferentes en un tiempo aproximado de dos horas. Debido a las seis disposiciones posibles de rotores, era necesario tener seis de las máquinas de Rejewski trabajando en paralelo: cada una de ellas representaba una de las posibles disposiciones. Ahora, con cada mensaje interceptado, se desarrollaba una tabla de relaciones para encontrar las cadenas resultantes, y con éstas se acudía al catálogo, encontrando la disposición de los rotores de la clave del día. Quedaba por resolver el problema del clavijero, así que Rejewski ingenió un método para obtener la configuración de éste: una vez conocida la disposición de los rotores, quitaba todos los cables y comenzaba a teclear el texto del mensaje. Al operar de este modo se obtenían frases sin sentido, puesto que se desconocía las conexiones del clavijero, pero de vez en cuando se obtenía un texto parecido a: "VULAR A MURICH". Se deducía fácilmente que esto querría decir "VOLAR A MUNICH", con lo que se veía que la U y la O estaban intercambiadas así como la R y la N. Con un número considerable de mensajes cifrados interceptados, era perfectamente posible deducir todas las posiciones del clavijero. Enigma había sido vencida nuevamente.

Una vez que tenía la clave del día poseía la misma información que el receptor a quien iba dirigido el mensaje y, por tanto, podía descifrar los mensajes con la misma facilidad. Los polacos interceptaron multitud de mensajes alemanes, con lo cual si no evitaban el peligro de invasión por parte de éstos, sí que podían ofrecer una idea de las pretensiones que el Tercer Reich tenía con respecto a Polonia.

[17] Diseño orig. de Rejewski (http://www.cryptomuseum.com/crypto/bombe/index.htm). 1. Rotores, 2. Motor eléctrico, 3. Interruptores (Cortesía de Janina Sylwestrzak, hija de Rejewski). Este concepto fue posteriormente desarrollado por los miembros del Servicio de

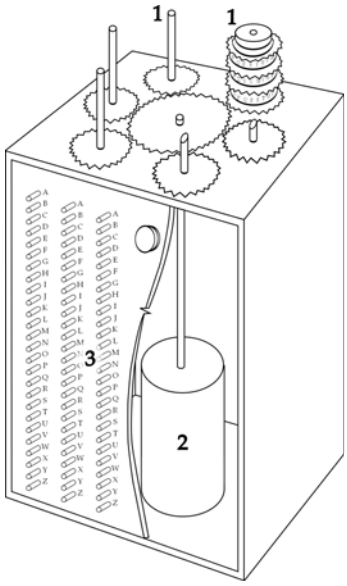

FIG. 11. Bomba criptológica.[17]

La inteligencia polaca, mantuvo constantemente informado a su gobierno a través del trabajo realizado por el BS4, lo que les hizo poner sobre aviso a la opinión internacional de las pretensiones invasoras de HITLER para con Polonia. Muy a su pesar, los aliados no tomaron en demasiada consideración estos avisos. Además los acontecimientos no hacían más que empeorar la maltrecha situación de los polacos ya que el 15 diciembre de 1938, los militares nazis, conscientes del origen comercial de Enigma, consideraron oportuno suministrar a los operadores de comunicaciones dos nuevos rotores además de los 3 rotores con los que ya contaba la máquina, lo cual aumentaba enormemente el rango de disposiciones de los mismos, exactamente a la enorme cantidad de $1,59 \times 10^{20}$. En lugar de tener 6 disposiciones distintas de los rotores, ahora se tenían 60, lo cual significaba para los polacos tener que construir 54 máquinas nuevas para poder hacer frente a este nuevo reto, que de tenerlas (opción esta ni remotamente probable ya que no tenían presupuesto para ello) aumentaría el tiempo de obtención de las claves en gran medida. Además, el 1 de enero de 1939, los alemanes aumentaron el número de cableado del clavijero hasta 10,

Inteligencia Británica (SIS) en Bletchley Park. Se trataba de una invención más desarrollada que el ciclómetro. Según parece su nombre fue acuñado debido al sonido *"tic-tac"* que éstas emitían cuando probaban las distintas posiciones de los rotores. Otra versión afirma que a REJEWSKI le vino la inspiración de las máquinas cuando estaba en una cafetería comiendo una bomba, un helado con forma de hemisferio. Las bombas mecanizaron eficazmente el proceso de descifrado. Significaba una respuesta natural a la Enigma, que era una mecanización de la codificación.

provocando un efecto devastador en las labores criptoanalíticas polacas. Todo este cúmulo de acontecimientos dejó a los polacos en una situación de aislamiento ciertamente preocupante lo cual les condujo inexorablemente a buscar ayuda. Sin demasiadas alternativas, la inteligencia polaca no tuvo más remedio que recurrir a sus aliados franceses, con la esperanza de que sus mayores recursos les permitieran aprovechar los avances polacos y sacar un mayor partido al concepto de la *bomba*. Enigma recuperaba virtualmente su inviolabilidad.

3. Huida, exilio o muerte

3.1. La búsqueda de aliados. La nueva invulnerabilidad de la Enigma resultó ser devastadora para los designios de Polonia, ya que Enigma no era exclusivamente un medio de comunicación, sino un instrumento fundamental en lo que HITLER acuñó como *blitzkrieg* («guerra relámpago»), que implicaba un ataque de la Wehrmacht rápido, intenso y coordinado. Por ello, la comunicación rápida y segura entre las diferentes tropas debía estar protegida, y Enigma significaba un inmejorable aval para garantizar gran parte del éxito de las acciones bélicas consideradas. Si los polacos no podían descifrar la Enigma, no tenían ninguna esperanza de detener una violenta invasión que obviamente tenía todos los visos de producirse de manera inminente tal y como avanzaban los acontecimientos.

FIG. 12. Enigma en acción.[18]

[18] a) Puesto de mando con radio a bordo de un Sd.KFz 251 del general de la 2ª División Panzer Heinz Guderian. Invasión de Francia (Mayo - 1940). Foto: Erich Borchert, Deutches Bundesarchive (Archivo Federal Alemán). Signatura: Bild+101I-769-0229-10A. http://www.bild.bundesarchiv.de/. b) Enigma con tres operadores. Uno de ellos realizaba los ajustes y tecleaba el mensaje. Otro anotaba las letras que aparecían en el panel luminoso

FIG. 13. Protagonistas de la reunión de Pyry.[19]

El 9 de enero de 1939, GUSTAVE BERTRAND organizó una infructuosa reunión de dos días en París entre criptólogos polacos, franceses y británicos. Los polacos, representados por el teniente coronel GWIDO LANGER, deseaban estrechar lazos de cooperación con los británicos visto que la amenaza de la guerra se cernía sobre ellos. Sin embargo no estaban dispuestos a revelar sus logros aún. A mediados de julio de 1939, cuando la invasión alemana de Polonia parecía inminente, el general jefe del ejército polaco, WACLAW STACHIEWICZ, autorizó al Biuro Szyfrów a compartir con los aliados todos los conocimientos técnicos sobre el descifrado de Enigma. El 24 de julio, ALFRED DILLWYN KNOX, jefe de los criptoanalistas británicos en la Oficina Exterior (Foreing Office), organizó una reunión a la que asistieron británicos y franceses. Viajaron a Pyry en

y el último llevaba a cabo la codificación en morse. En el lugar de recepción se necesitaban el mismo número pero las operaciones eran a la inversa que en el lugar de emisión. Foto cortesía de Helge Fykse, http://fykse.dnsalias.com/bilder/enigma/.

[19] De izq. a drcha y de arriba a abajo: 1. GUSTAVE BERTRAND [6], 2. ALASTAIR DENNISTON (http://enigma.umww.pl/index.php?page=Denniston), 3.MAKSYMILIAN CIĘŻKI (http://wyborcza.pl/51,75248,5980398.html?i=0), 4. ALFRED DILLWYN KNOX (http://enigma.umww.pl/index.php?page=dillwyn-knox), 5. WILFRED DUNDERDALE (http://bondambitions.com/2011/01/origins-of-bond) y 6. STEWART MENZIES (http://www.reformation.org/spies-are-despicable.html).

los bosques de Kabackie, cerca de Varsovia, para reunirse en un viejo búnker, que resultaba ser el centro neurálgico del ataque polaco al código enigma. En el equipo británico figuraba el comandante Alastair Denniston, jefe de las operaciones criptográficas en Bletchley Park (cuyo nombre en clave era "Station X" - Estación X-), una mansión campestre a unos 70 kms al noroeste de Londres, y el comandante Humphrey Sandwich. A. Denniston era un reconocido defensor de la importancia de las matemáticas en la lucha criptoanalítica, de hecho gran parte del posterior éxito en Bletchley Park se debe a que fue uno de los que apostó por enrolar en esta lucha a las mejores mentes matemáticas y lógicas del momento en Gran Bretaña. Los franceses estaban representados por el comandante Gustave Bertrand, y el capitán Henri Braquenié. Finalmente los polacos estaban representados por el capitán Maksymilian Ciężki, el teniente coronel Gwido Langer y el coronel jefe Stefan Mayer. Estas conversaciones sirvieron para que los aliados se pusieran al día de todos los avances logrados por el BS4. El 16 de agosto de 1939, mientras los jóvenes de Reino Unido respondían masivamente a la llamada de alistamiento, el comandante G. Bertrand llegaba a la Estación de Victoria acompañado del comandante Wilfred Dunderdale de la inteligencia británica en París. Bertrand portaba un maletín con información fundamental en la guerra contra Enigma, además de una réplica de la misma (una *bomba* ya prometida por los polacos en su reunión en Pyry) que entregó al general Stewart Menzies, 2º jefe del Servicio de Inteligencia Británico. Dos semanas después, Hitler invadía Polonia y estallaba la 2ª Guerra Mundial.

3.2. La cruzada final polaca. Tras la invasión de Polonia por los nazis, una gran cantidad de miembros del BS4 fueron capturados, torturados y asesinados. Afortunadamente, Rejewski, Różycki y Zygalski pudieron abandonar el país y poner rumbo a Rumanía antes de ser capturados. Cuando llegaron a la capital dacia intentaron sin éxito solicitar asistencia en la Embajada Británica. Sin embargo la Embajada Francesa sí que se la proporcionó, evacuándolos a París a finales de septiembre de 1939.

Por otro lado la Unión Soviética también invadió Polonia el 17 de septiembre de 1939, por lo que el Biuro Szyfrów decidió destruir de forma inmediata toda la documentación acerca de Enigma.

El centro de inteligencia franco-polaca se estableció en octubre de 1939 en el Château de Vignolles, en Gretz-Armainvillers, a 40 kms al noreste de París, recibiendo el nombre secreto de "Bruno"[20]. El centro se dedicó a interceptar transmisiones de radio alemanas en coordinación con el GC&CS británico (Escuela Gubernamental de Códigos y Cifras). De manera adicional, siete criptólogos españoles republicanos fueron empleados en Bruno con el fin de poder descifrar códigos de la Italia fascista y la España franquista.

[20] Es posible encontrar que algunos autores lo denominan "PC Bruno", donde PC significa "Puesto de Mando".

El principal trabajo del centro era alertar a los Aliados acerca de la inminente invasión de Francia por las tropas germanas. En mayo de 1940, Alemania comenzó su invasión, y a mediados de junio había llegado a París. El 10 de junio de ese año, la unidad Bruno recibió ordenes de evacuar, y en 48 horas Rejewski y sus colegas, además de los criptólogos españoles liderados por Faustino Antonio Camazón Valentín, ponían rumbo en un viaje que duraría 10 días que les llevaría a Toulouse, a Orán en el norte de África y finalmente al centro de operaciones denominado Villa Kouba que los franceses tenían cerca de Argel. París cayó el 14 de junio, y el 22 Francia firmaba su rendición parcial (parte del país, que más tarde acuñría el nombre de la Francia de Vichy, no era ocupada y se le permitía cierta autonomía).

Sin embargo, lejos de arrugarse, los criptólogos polacos y españoles, denominados "Equipo Z" y "Equipo D" respectivamente, decidieron continuar con su peligrosa tarea. El mayor Gustave Bertrand regresó en septiembre a Francia y fue entonces cuando los integrantes de Bruno decidieron crear una nueva unidad encubierta denominada "Cadix", en el Château des Fouzes, en Uzès, cerca de Nimes, al sur de la Francia de Vichy, entre Montpellier y Avignon. Para evitar cualquier sospecha Rejewski se empleó como profesor de matemáticas en Nantes.

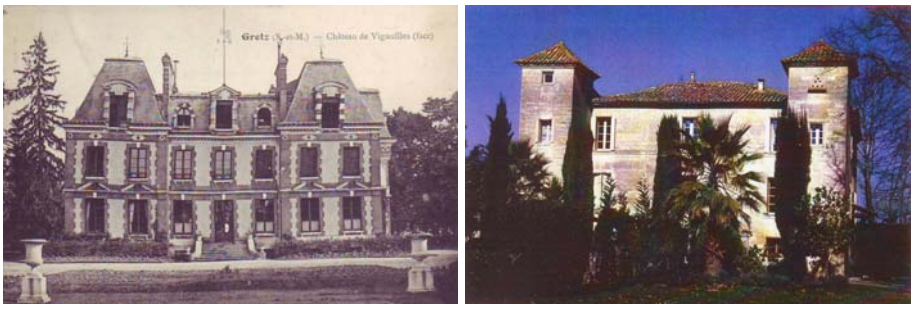

Fig. 14. Château de Vignolles[21]y Château des Fouzes [6].

[21] http://pmcdn.priceminister.com/photo/858066849.jpg

[22] De izq. a drcha: 1. Henri Braquenié, 2. Piotr Smoleński, 3. Edward Fokczyński, 5. Maksymilian Ciężki, 7. Gwido Langer, 8. Mary Bertrand, 9. Gustave Bertrand, 13. Henryk Zygalski (detrás, con gafas), 14. Jan Graliński, 18. Jerzy Różycki. 20. Marian Rejewski. http://www.ww2.pl/ww2/zdjecia/153.jpg

[23] (a) De izq. a drcha.: 1. Henryk Zydalski, 2. Jercy Różycki, 3. Marian Rejewski. (b) Junto a criptógrafos españoles. De izq. a drcha: 1. Marian Rejewski, 2. Edward Fokczyński, 3. español no identificado, 4. Henryk Zygalski, 5. español no identificado, 6. Jerzy Różycki; 7. Faustino Antonio Camazón Valentín, 8. Antoni Palluth, 9. español no identificado. http://en.wikipedia.org/wiki/File:Zygalski-rozycki-rejewski.jpg, http://www.ugr.es/ aquiran/cripto/museo.htm

Fig. 15. Trabajadores del centro polaco-hispano-francés de radioespionaje "Cadix" (1940-1942).[22]

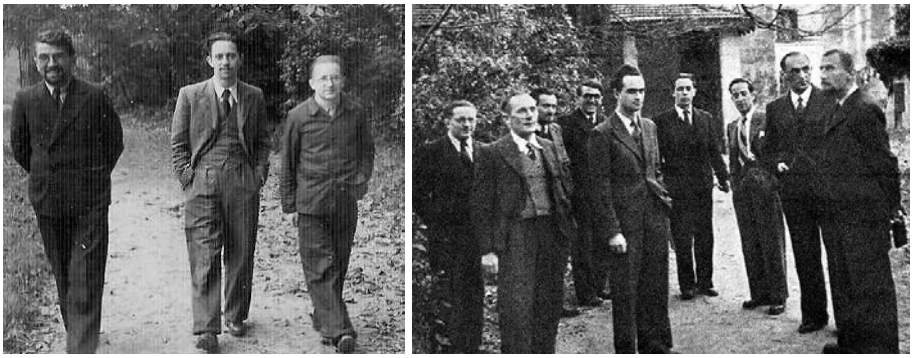

Fig. 16. Imágenes en los jardines del Château des Fouzes en algún momento entre septiembre de 1940 y junio de 1941.[23]

La madrugada del 9 de junio de 1942, mientras regresaba al centro de Cadix de un viaje a la oficina de Château Couba en Argel que estaba dirigida por Maksymilian Ciężki, el barco de Jercy Ròżycki de nombre Lamoricière, se vio sorprendido por un fuerte temporal cuando estaba a 30 millas al norte de la isla de Menorca. Cuando remontaba hacia Marsella por el Canal de Menorca, el buque ya llevaba ocho horas de retraso y se enfrentaba a un temporal con olas de hasta once metros. Aún así, el capitán decidió virar hacia el sur de Menorca

con el fin de socorrer al carguero Jumiéges. Al llegar a las coordenadas del carguero, sobre las 3 de la madrugada, la tripulación comprobó que el Jumiéges ya se había hundido. Atrapados en el temporal, el capitán del Lamoriciére ordenó recuperar el rumbo pero al parecer había entrado agua por las compuertas de cubierta que provocó la parada de dos motores del buque. Cuando el capitán consideró que sería imposible llegar a su destino en el puerto de Marsella, decidió buscar refugio. Sin embargo, no tuvo éxito en su maniobra, y el barco fue engullido literalmente por las olas y naufragó. No obstante algunos investigadores ponen de manifiesto que este hecho pudiera no haber sido únicamente un trágico accidente. Su argumentación es que las circunstancias en torno a este naufragio no son demasiado claras. Parece ser que en medio del temporal el capitán intentó girar el barco de 112 metros de eslora para buscar refugio en la costa sur de la isla de Menorca. En esta maniobra la tramontana golpeó violentamente el costado y la carga de naranjas que llevaba en sus bodegas se soltó y golpeó fuertemente contra el casco que resultó gravemente dañado, además de desplazar el centro de gravedad del buque provocando que éste se escorara hacia un costado. Desafortunadamente parece ser que el agua que entraba apagó los motores restantes y el generador eléctrico, con lo que las bombas de achique no funcionaron. Este cúmulo de desafortunados hechos sugiere la sospecha de que se pudiera haber producido un sabotaje. Ante esta situación, el capitán ordenó que tripulantes y pasajeros recolocaran la carga desplazada para que el barco se estabilizara pero todo fue inútil. No parece una casualidad tampoco que entre los 301 pasajeros que perdieron la vida en el suceso (únicamente hubo 93 supervivientes), se encontraran varios criptólogos fundamentales en el trabajo contra el código Enigma, como los polacos Piotr Smolesński, y el capitán Jan Graliński, de la Sección Rusa del Biuro Szyfrów, además del propio Jercy Ròżycki, y el oficial francés que acompañaba a los tres polacos, el capitán François Lane.

En noviembre de 1942, mientras los aliados preparaban la invasión del norte de África, las tropas alemanas ocuparon la Francia de Vichy. La unidad secreta en el Château des Fouzes corría un grave peligro de ser descubierta y desmantelada, por lo que sus miembros debieron ser evacuados de manera fulminante. Todo el personal escapó el 9 de noviembre justo a tiempo, ya que tres días después los alemanes descubrían la operación secreta de Cadix. Rejewski y Zygalski no tuvieron más remedio que abandonar el país vía España, pero al cruzar los Pirineos fueron arrestados y encarcelados primero en la prisión de La Seu d'Urgell y después en la de Lleida. El 4 de mayo serían liberados gracias a la intermediación de la Cruz Roja polaca y enviados a Madrid. El 21 de julio salían de Madrid con rumbo a Portugal. Finalmente llegaron a Londres vía Gibraltar el 3 de agosto de 1943. Allí, paradojas de la vida, no fueron invitados a colaborar con el proyecto que lideraba entre otros el genio matemático de Alan Turing en Bletchley Park, que era el centro neurálgico de

[24] http://en.wikipedia.org/wiki/File:Gralinski,_Rozycki_and_Smolenski.jpg

FIG. 17. De izqda. a drcha.: 1. JAN GRALIŃSKI, 2. JERCY RÒŻYCKI, 3. PIOTR SMOLESŃSKI, en Cadix.[24]

la lucha aliada contra el código Enigma, sino que ocuparon puestos menores en oficinas de cifra y código secundarias, digamos de 2ª división, en Boxmoor, cerca de Hemel Hempstead, lo cual no deja de resultar sorprendente, dado que realmente los aliados habían necesitado antes de sus avances para comenzar a desarrollar las máquinas bombe. Sin embargo no todos los polacos corrieron la misma suerte que REJEWSKI y ZYGALSKI. Un grupo de polacos miembros del equipo Cadix, entre ellos GWIDO LANGER, MAKSYMILIAN CIĘŻKI, ANTONI PALLUTH, EDWARD FOKCZYŃSKI y KAZIMIERZ GACA intentaron escapar cruzando la frontera con España, pero fueron arrestados en Prats de Mollo en un control policial. Tras un mes fueron liberados e intentaron nuevamente entrar en España varias veces sin éxito. Sin noticias de BERTRAND, decidieron arriesgarse a cruzar los Pirineos en un último intento guiados por un contrabandista. Fueron traicionados por éste que colaboraba con la Gestapo, y capturados por los alemanes cuando intentaban cruzar la frontera la noche del 10 al 11 de marzo de 1943. A pesar de ser interrogados y torturados con gran brutalidad por la policía alemana de Perpiñán, ninguno de ellos reveló información alguna sobre Cadix. LANGER y CIĘŻKI fueron enviados al campo de prisioneros 122 en Compiégne, Francia, y el 9 de septiembre al campo de concentración alemán de las SS *Sonderkommando Schloss Eisenberg* en Checoslovaquia, donde sobrevivieron en condiciones deplorables. PALLUTH, FOKCZYŃSKI y GACA fueron enviados a Alemania a campos de prisioneros de guerra y trabajos forzados. PALLUTH murió al estallar una bomba durante un ataque aéreo aliado y FOKCZYŃSKI finalmente no pudo aguantar y murió de agotamiento. Ambos murieron en el campo de concentración de Sachsenhausen, cerca de Berlín.

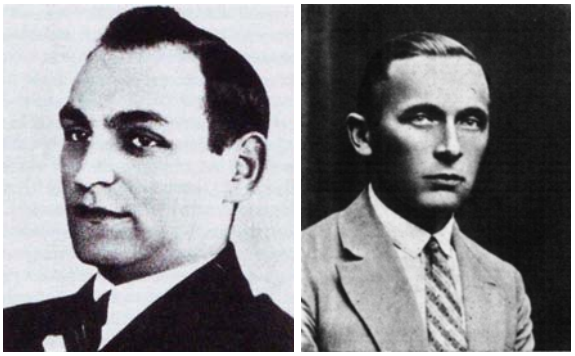

FIG. 18. A. PALLUTH y E. FOKCZYŃSKI [6].

En mayo de 1945, LANGER, CIĘŻKI y GACA fueron liberados por las tropas estadounidenses. Los últimos años de LANGER no fueron nada fáciles. BERTRAND y gran parte de oficiales polacos le dieron la espalda a pesar de la interpelación a su favor de CIĘŻKI. Herido en su orgullo siempre defendió que siguieron las vías de escape establecidas por la inteligencia francesa para evitar ser capturados por los alemanes, sin embargo BERTRAND siempre le responsabilizó directamente del desacierto de la operación de evacuación. Según posteriores testimonios de oficiales de la inteligencia francesa durante la guerra, parece evidente que no se siguieron los mejores procedimientos en la evacuación, ya que en aquel momento existían vías para cruzar a España completamente seguras que no fueron utilizadas. Con estas revelaciones parece evidente deducir que los polacos fueron en cierto modo abandonados a su suerte. LANGER murió en el campo del ejército polaco en Kinross, Escocia, el 30 de marzo de 1948. CIĘŻKI permaneció hasta su muerte en Gran Bretaña, donde al contrario que LANGER, obtuvo muchas condecoraciones militares. Murió el 9 de noviembre de 1951.

En noviembre de 1946 REJEWSKI retornó a Polonia donde le esperaban su mujer y sus dos hijos. Una vez allí le fue muy complicado encontrar un puesto de docente por lo que finalmente aceptó una oferta como contable en Bydgoszcz, su ciudad natal, al norte de Polonia. Mantuvo bajo juramento su promesa de no revelar a nadie ninguna de sus actividades contra los códigos alemanes, manteniendo en estricto secreto todos sus avances con respecto a la máquina Enigma. El 12 de agosto de 1978, en reconocimiento a su labor criptoanalítica, el Gobierno polaco le concedió la Cruz de los Oficiales de la Orden de la Refundación de Polonia. Murió de un ataque al corazón el 13 de febrero de 1980 tras sufrir una larga enfermedad coronaria. Hoy día es considerado como un auténtico héroe nacional y se le han dedicado varios monumentos en su recuerdo.

[25] http://commons.wikimedia.org/wiki/File:Bydgoszcz_Rejewski_3.jpg?uselang=pl

FIG. 19. Estatua de bronce de REJEWSKI en Bydgoszcz, en conmemoración del centenario de su nacimiento (2005).[25]

Por su parte, tras la guerra, ZYGALSKI permaneció exiliado en el Reino Unido donde trabajó como profesor de estadística matemática en la Universidad de Surrey hasta su retiro, y al igual que REJEWSKI tuvo que mantener en secreto todos sus trabajos sobre criptografía. Murió el 30 de agosto de 1978 en Liss, donde fue incinerado y sus cenizas fueron llevadas a Londres. Poco antes de su muerte recibió el doctorado honorario de la Universidad Polaca en el Exilio por sus logros conseguidos contra el código Enigma.

Referencias

[1] F. L. BAUER. *Decrypted Secrets. Methods and Maxims of cryptology*, 4th ed. Springer–Verlag: Berlin, 2007.

[2] R. CEANO. *La máquina Enigma*. `http://www.kriptopolis.com/enigma, 2012.`

[3] C. CHRISTENSEN, *Polish mathematicians finding patterns in enigma messages*, Mathematics Magazine no. 80, (2007), 247–273.

[4] A. KERCKHOFFS. *La cryptographie militaire*, Journal des sciences militaires. **IX** (1883), 5–83.

[5] W. KOZACZUK. Enigma: *The Key to the Secrets of the Third Reich 1933–45*. Interpress, 1984.

[6] JEAN MEDRALA. *L'enigme polonaise en résistance á Uzés 1940–1942. Une aventure humaine prestigieuse et dramatique*. Conférence Enigma: S'il te plait dessine-moi la Pologne (Paris), 2008.

[7] A. R. MILLER. *The Criptographic Mathematics of Enigma*. Center for Cryptologic History, 1996.

[8] J. J. ORTEGA TRIGUERO, M. A. LÓPEZ GUERRERO & E. C. GARCÍA DEL CASTILLO CRESPO. *Introducción a la criptografía. historia y actualidad*. Colección Monografías, no. 50, 2006.

[9] A. Quirantes Sierra. *Enigma: la solución polaca (i) y (ii)*. Boletín del Taller de Criptología no. 18 (2003).
[10] M. Rejewski. *An application of the theory of permutations in breaking the Enigma cipher*. Applicationes Mathematicae **16** (4) (1980).
[11] M. Rejewski. *How Polish Mathematicians deciphered the Enigma*. Annals of the History of Computing **3** (3) (1981).
[12] J. M. Sánchez Muñoz. *Nazis y matemáticas*. 2ª Jornada Internacional "Matemáticas Everywhere" (Castro Urdiales), Grupo de Innovación Educativa "Pensamiento Matemático", Universidad Politécnica de Madrid, junio 2012.
[13] S. Singh. *Los códigos secretos: El arte y la ciencia de la criptografía, desde el antiguo Egipto a la era internet*. Editorial Debate, 2000.
[14] S.Wesolkowski. *The Invention of Enigma and how the Polish broke it before the start of WWII*. IEEE Conference on the History of Telecommunications (Canada), University of Waterloo, 2001.

(Recibido en diciembre de 2012. Aceptado para publicación en marzo de 2013)

José Manuel Sánchez Muñoz
Grupo de Innovación Educativa "Pensamiento Matemático"
Universidad Politécnica de Madrid
calle Profesor Aranguren s/n, Madrid, España
e-mail: jmanuel.sanchez@gmx.es