Historias de Matemáticas

Criptología Nazi. Los Códigos Secretos de Hitler

Nazi Cryptology. Hitler's Secret Codes

José Manuel Sánchez Muñoz

Revista de Investigación

Volumen III, Número 1, pp. 059–120, ISSN 2174-0410
Recepción: 23 Nov'12; Aceptación: 6 Feb'13

1 de abril de 2013

Resumen

Este artículo trata la importancia de la desencriptación de los Códigos Enigma y Lorenz alemanes por parte de los aliados gracias al trabajo analítico de multitud de matemáticos, cuyo resultado fue vital para la derrota de los nazis en la 2ª Guerra Mundial, acortando ésta al menos en dos años.

Palabras Clave: Nazis, Matemáticas, 2ª Guerra Mundial, criptología, Enigma, Bomba, Lorenz, Colossus, Bletchley Park.

Abstract

This article considers the importance of the German Enigma and Lorenz codes cracking by the allies through the analitical work developed by many mathematicians, which had vital consequences for the nazi defeat in the 2nd World War, shortening it by around two years.

Keywords: Nazis, Mathematics, World War Two, criptology, Enigma, Bombe, Lorenz, Colossus, Bletchley Park.

1. Breve evolución histórica de la criptología hasta la 2ª Guerra Mundial

A lo largo de la historia, el hombre ha sentido la necesidad de codificar sus mensajes con la mera intención de que estos pasaran inadvertidos a los ojos de curiosos y mantener intacto el secretismo de los mismos. Surgieron así los primeros mensajes ocultos primitivos que rápidamente encontraron un nicho de utilidad en aquellas comunicaciones cuya privacidad debía ser garantizada. A esta comunicación secreta lograda mediante la ocultación se la denomina *esteganografía*, derivada del *steganos* o "encubierto" y *graphein* o "escribir". La principal desventaja de esta ciencia era que cualquiera podría interceptar un mensaje oculto y comprometer la seguridad de la comunicación.

Paralelamente a la *esteganografía*, surgió la ciencia de la *criptografía*, del griego *kryptos* o "escondido", cuya finalidad consistía más que en ocultar el mensaje, ocultar su significado mediante un proceso de codificación. De forma añadida surgieron las primeras técnicas de análisis cuya

finalidad principal consistía en desenmascarar el contenido secreto de los mensajes cifrados, lo que se denominó *criptoanálisis*. La evolución de las técnicas criptográficas supuso el avance y desarrollo de nuevas técnicas de análisis críptico.

Desde su inicio, la criptografía encontró su principal utilidad en el arte de la guerra. Algunos de los testimonios más antiguos que narran la utilización de escrituras secretas se remontan a Herodoto que escribió una crónica acerca de los conflictos entre Grecia y Persia en el siglo V a.C. Gracias a la mera ocultación de un mensaje de aviso del griego Demarato que vivía en la ciudad persa de Susa, donde se revelaban los planes estratégicos de invasión del archipiélago heleno del líder persa Jerjes, Grecia tomó una clara ventaja y pudo hacerse con la victoria y evitar la invasión en el año 480 a.C.

Los métodos criptográficos se pueden clasificar en métodos de encriptación *simétricos* y *asimétricos*. En los primeros se utiliza la misma clave para cifrar y descifrar los mensajes encriptados, al contrario que los segundos que utilizan diferentes claves. Los métodos *asimétricos* nacieron a finales del siglo XX y revolucionaron la ciencia de la criptografía. Dentro de los *métodos simétricos* de cifrado podemos encontrar los métodos de *sustitución* y *transposición*.

1.1. Métodos de Sustitución

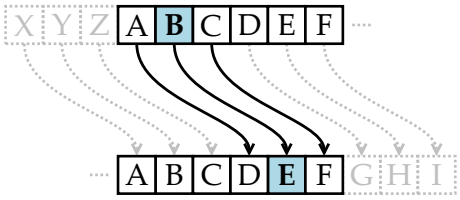

Figura 1. Cifrado de César

El primer ejemplo documentado de un *método de sustitución* de encriptación fue utilizado por Julio César en *La guerra de las Galias*, para enviar un mensaje a Cicerón que estaba sitiado y a punto de rendirse, sustituyendo las letras romanas por griegas haciendo ininteligible el mensaje. Para cifrar un mensaje mediante el *Cifrado de César*, cada letra de dicho mensaje era reemplazada con la letra de tres posiciones después en el abecedario. Por tanto, la A sería reemplazada por la D, la B por la E, la C por la F, y así sucesivamente. Por último la X, la Y y la Z serían reemplazadas por la A, la B y la C respectivamente. De ahí, que por ejemplo, "ATACAR" se cifraría como "DWDFDU". César rotaba el abecedario de tres en tres letras pero en general funcionaba con cualquier número acordado entre el emisor y el receptor del mensaje.

Figura 2. Sello conmemorativo sirio de Al Kindī (1994).[1]

Durante siglos este tipo de cifrado monoalfabético se consideró prácticamente imposible de romper, sin embargo con el paso del tiempo surgieron las técnicas de análisis criptográfico nacidas en el seno de la civilización musulmana. Aunque no se conoce el autor originario de la *técnica de análisis de tablas de frecuencia*, parece que al final del siglo IX d.C., Abũ Yũsuf Ya'qũb ibn Ishũq Al Kindī (801-873), conocido como *el filósofo de los árabes*, fue el primero en documentar dicho análisis en su libro *Sobre el descifrado de mensajes criptográficos* descubierto de forma casual en el Archivo de Estambul en 1987. Al Kindī que trabajó en filosofía, astrología, astronomía, cosmología, química, lógica, matemática, música, medicina, física, psicología y meteorología, manifestaba en dos breves párrafos:

> *"Una manera de resolver un mensaje cifrado, si sabemos en qué lengua está escrito, es encontrar un texto llano diferente escrito en la misma lengua y que sea lo suficientemente largo para llenar alrededor de una hoja, y luego contar cuántas veces aparece cada letra. A la letra que aparece con más frecuencia la llamamos «primera», a la siguiente en frecuencia la llamamos*

[1] http://jeff560.tripod.com/stamps.html

> *«segunda», a la siguiente «tercera», y así sucesivamente, hasta que hayamos cubierto todas las letras que aparecen en la muestra de texto llano.*
>
> *Luego observamos el texto cifrado que queremos resolver y clasificamos sus símbolos de la misma manera. Encontramos el símbolo que aparece con más frecuencia y lo sustituimos con la forma de la letra «primera» de la muestra de texto llano, el siguiente símbolo más corriente lo sustituimos por la forma de la letra «segunda», y el siguiente en frecuencia lo cambiamos por la forma de la letra «tercera», y así sucesivamente, hasta que hayamos cubierto todos los símbolos del criptograma que queremos resolver."*

La técnica de Al Kindī consiste en examinar un fragmento extenso de texto normal, o quizás varios, para establecer la frecuencia de cada letra del alfabeto. En castellano, dicha frecuencia se ve representada por la Tabla 1. A continuación, es necesario examinar el texto cifrado y determinar la frecuencia de cada letra. Si la letra más corriente en el texto cifrado es, por ejemplo, la J, entonces parecería probable que sustituyera a la E (que es la más comúnmente utilizada en español). Y si la segunda letra más frecuente en el texto cifrado es la P, probablemente sustituya a la A, y así sucesivamente. La técnica de Al Kindī, conocida como *análisis de frecuencia*, muestra que no es necesario revisar cada una de las billones de claves potenciales. En lugar de ello, es posible revelar el contenido de un mensaje codificado analizando simplemente la frecuencia de los caracteres en el texto cifrado, y realizando una comparativa con la tabla de frecuencias de un texto en el idioma considerado.

Tabla 1. Frecuencias de caracteres en castellano.[2]

Frecuencia Alta		**Frecuencia Media**		**Frecuencia Baja**	
Letra	**Porcentaje**	**Letra**	**Porcentaje**	**Letra**	**Porcentaje**
E	13,68	C	4,68	Q	0,88
A	12,53	T	4,63	H	0,70
O	8,68	U	3,93	F	0,69
S	7,98	M	3,15	Z	0,52
R	6,87	P	2,51	J	0,44
N	6,71	B	1,42	Ñ	0,31
I	6,25	G	1,01	X	0,22
D	5,86	V	0,90	W	0,02
L	4,97	Y	0,90	K	0,01

1.2. Métodos de Transposición

Tras el análisis de frecuencia, la criptografía continuó su avance surgiendo entonces nuevos métodos simétricos de encriptación cada vez más y más sofisticados, denominados *Métodos de Transposición*, que consisten como su definición indica en transponer los textos, es decir que ahora no son las letras las que cambian, sino su orden.

Pongamos un ejemplo; imaginemos que tanto el emisor del lenguaje cifrado como el receptor consideran en principio un número menor de nueve dígitos como clave, por ejemplo el 231[3]. Dicha clave ponía de manifiesto que el texto debía ser escrito en tres columnas (en principio sin considerar espacios entre palabras). De este modo el emisor codificaría la frase "DESEMBARCAR AL AMANECER",

[2] FLETCHER, P., *Secret and Urgent: the Story of Codes and Ciphers*, pp. 254-255, Blue Ribbon Books, 1939.

[3] En ocasiones se utilizaban como clave letras del alfabeto, de tal modo que si a la A le corresponde el 1, a la B el 2 y así sucesivamente, si se hacía uso por ejemplo la palabra EVA, la clave de codificación se correspondía al número 5-23-1, codificado de texto de tres columnas, en la que la primera ha de colocarse en el tercer grupo de letras del mensaje cifrado, la segunda en el grupo inicial de dicho mensaje, y la tercera en el segundo grupo del mensaje.

1	2	3
D	E	S
E	M	B
A	R	C
A	R	A
L	A	M
A	N	E
C	E	R

$\Rightarrow$

2	3	1
E	S	D
M	B	E
R	C	A
R	A	A
A	M	L
N	E	A
E	R	C

$\Rightarrow$ "EMRRANE SBCAMER DEAALAC"

De esta forma el receptor recibía dicho mensaje y colocaba dicho grupo de letras en tres columnas, de modo que el primer grupo de letras correspondía con la segunda columna del lenguaje original, el segundo se correspondía con la tercera columna, y el tercer grupo se correspondía con la primera columna.

1.3. El Disco de Alberti

Durante siglos, la cifra de sustitución monoalfabética simple había resultado lo suficientemente complicada para garantizar su indescifrabilidad. Sin embargo las técnicas de análisis de frecuencias desarrolladas por Al Kindī fueron rápidamente transmitidas al mundo occidental, comprometiendo seriamente la integridad de los mensajes cifrados. Comenzaba a ser evidente que la batalla entre los criptógrafos y los criptoanalistas estaba comenzando a ser ganada por el segundo grupo. Es así cuando en torno a 1460, el erudito renacentista natural de Florencia, Leon Battista Alberti (1404-1472) comenzó a trabajar en una nueva técnica de cifrado de mensajes. Mientras gozaba de una conversación durante un paseo por el Vaticano, su amigo, y a la sazón secretario pontificio, Leonardo Dato, puso al corriente a Alberti de los últimos adelantos en cuanto a criptografía se refería. Esta conversación fortuita animó a Alberti a investigar, llegando a la conclusión de que era necesario utilizar dos o más alfabetos cifrados, alternando entre ellos durante la codificación con el fin de fortalecer la encriptación y confundir así a los potenciales criptoanalistas.

De 1466 a 1467 escribió su tratado *De Componendis Cyphris*, considerado como el escrito sobre criptología más antiguo del mundo occidental. En dicho tratado explica el desarrollo de las técnicas polialfabéticas. A partir de ahí, Alberti analiza diversos procedimientos: sustituciones de tipos diferentes, transposiciones de letras dentro de palabras y mensajes obtenidos marcándose las posiciones de ciertas letras en un texto inocente. Finalmente concluye su introducción con la descripción de su invención, *el disco cifrante*, también conocido como *Disco de Alberti*.

> *"Fijo dos discos en una placa de cobre. Uno, el mayor, será fijo y el otro, el menor, movible. El diámetro del disco fijo es superior en un noveno al del disco móvil. Divido la circunferencia de cualquiera de los dos en veinticuatro partes iguales llamadas sectores. En cada uno de los sectores del disco grande escribo en orden alfabético normal una letra mayúscula roja: primero A, a continuación B, después C, etc, omitiendo H y K que no son indispensables."*

De este modo, Alberti obtuvo un total de 20 letras, pues J, U, W e Y tampoco figuraban en su alfabeto. En los cuatro sectores restantes escribió los números 1, 2, 3 y 4. Haciendo referencia a los veinticuatro sectores del disco pequeño escribió:

> *"...una letra minúscula, en negro, no en la orden normal como en el disco fijo, pero en una orden incoherente. De esta forma, se puede suponer que la primera letra será a, la décima segunda g, la décima tercera q y así sucesivamente, de modo que todos los veinticuatro sectores sean llenados porque el alfabeto latino posee veinticuatro caracteres, siendo el vigésimo cuarto &. Efectuados estos arreglos, se coloca el disco pequeño sobre el grande, de modo que*

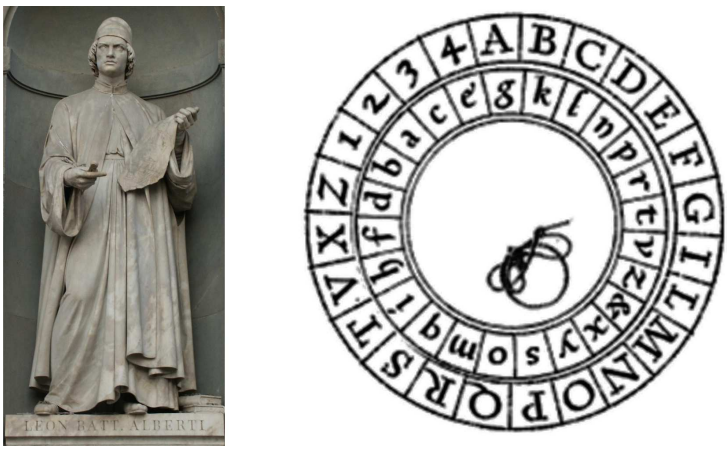

Figura 3. Estatua de Leon Battista Alberti en la Galería Uffizi, Florencia, y Disco de Alberti (imagen del manuscrito original "De Componendis Cyphris", 1466).

> *una aguja pasada por los dos centros sirva como un eje común alrededor del cual girará el disco móvil."*

Se considera una de las letras del disco móvil como letra llave o letra índice, por ejemplo k. Hecho esto el emisor alinea esta letra llave con cualquier letra del disco externo e informa de la posición del disco móvil al receptor escribiendo la letra escogida. Alberti usó el ejemplo de k alineada con B.

> *"Usando este punto de partida, cada letra del mensaje representará la letra fija por encima de ella. Después de escribir tres o cuatro letras, puedo cambiar la posición de la letra-índice de modo que k esté, por ejemplo, sobre D. Después, en mi mensaje, escribiré una D mayúscula y, a partir de este punto, k no significará más B y sí D, y todas las letras del disco fijo tendrán nuevas letras equivalentes."*

1.4. La Cifra Vigenère

Alberti puede ser considerado como el inventor del cifrado polialfabético y sus estudios sirvieron de base para trabajos posteriores como los de Johannes Trithemius que inventó *la tábula recta*, Giovanni Porta y sobre todo del diplomático francés de mediados del siglo XVI Blaise Vigenére (1523-1596), que a diferencia de Alberti utilizó la enorme cantidad de 26 alfabetos cifrados. Vigenère utilizó como base *la tábula recta* de Trithemius, y la amplió generando *la tábula de Vigenère*, que se muestra en la Tabla 2.

Figura 4. Blaise de Vigenère Bovrbonois (1515).[4]

Desde el punto de vista de su funcionamiento, se numeran las 26 letras del abecedario de forma que A = 0, B = 1, ..., Z = 25. En términos matemáticos puede expresarse como:

$$Y_i = (X_i + Z_i) \, mod \, T$$

donde T representa el número total de letras del alfabeto considerado (en general 26), X_i representa el ordinal de las letras de la palabra clave considerando las filas de la Tabla 2, es decir, que a P le

[4] Retrato de Thomas de Leu. Edificio Stephen A. Schwarzman. División de Arte, Pinturas y Fotografías Miriam e Ira D. Wallach.

Tabla 2. Tábula de Cifrado Vigenère

Llano	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
1	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	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
(5º) 4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
(1º) 13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
(2º) 14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
(3º) 17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
(4º) 19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	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

corresponde al numero 15 en modo horizontal, y Z_i representa el ordinal de la letra de texto plano (sin cifrar) considerada, que se corresponde con las columnas de la Tabla 2, esto es, la L en modo vertical le corresponde al numero 11. Finalmente Y_i representa el ordinal de la letra cifrada en el alfabeto considerado. Entonces la ecuación quedará de la siguiente manera $Y_i = (15 + 11)\ mod\ 26$. El resultado es 0, donde 0 es igual a A en modo horizontal. Haciendo uso de la Tabla 2, vamos a ilustrar cómo el emisor generaba un mensaje cifrado y el receptor descifraba dicho mensaje utilizando una codificación-descodificación por medio de una palabra clave. Imaginemos que el emisor quiere cifrar la orden *"movilizar las tropas dos km al sur"* considerando como clave la palabra "norte". La palabra "norte" especifica que se utilizará la codificación de los alfabetos 13, 14, 17, 19 y 4 en ese orden hasta finalizar el texto llano original. De este modo el emisor haría uso de la Tabla 2 y para la primera letra del mensaje original "m" se corresponde en el alfabeto 13 con la "Z", la segunda letra "o" se corresponde en el alfabeto 14 con la "C", la "v" se corresponde en el alfabeto 17 con la "M", la "i" se corresponde en el alfabeto 19 con la "B", y la "l" se corresponde en el alfabeto 4 con la "P", a partir de aquí el emisor continuaría con el proceso de encriptación volviendo a hacer uso de la secuencia de alfabetos 13, 14, 17, 19 y 4, y así sucesivamente. Con todo lo anterior el mensaje cifrado tendría el aspecto especificado en la Tabla 3.

El receptor del mensaje cifrado podría invertir el proceso de encriptado repitiendo la operación en la Tabla 2, entrando primero en el alfabeto 13 y mirando en el alfabeto llano que la "Z" se corresponde con la "m", la "C" del alfabeto 14 se corresponde en el alfabeto llano con la "o", y así sucesivamente.

Este sistema de cifrado tenía dos ventajas fundamentales respecto a los sistemas de encriptación conocidos hasta ese momento. La primera era que aparentemente resultaba inexpugnable al análisis de frecuencias, ya que una misma letra no tenía porqué repetir un patrón de re-

Tabla 3. Encriptación de mensaje mediante el Cifrado de Vigenère (I).

Texto Llano Orig.	m o v i l i z a r l a s t r o p a s d o s k m a l s u r
Clave	N O R T E N O R T E N O R T E N O R T E N O R T E N O R
Texto Cifrado	Z C M B P V N R K P N G K K S C O J W S F Y D T P F I I

petición, y aparecía cifrada con diferentes letras. La segunda era la enorme combinación de posibilidades a barajar. Todas estas ventajas tendrían que haber sido suficientes para que todos los secretarios de cifra de Europa hubieran adoptado este método como sistema oficial de encriptación, sin embargo esta cifra, a todas luces perfecta, permanecería prácticamente ignorada durante los dos siglos y medio posteriores, seguramente debido a la complejidad de su aplicación a nivel práctico, que supondría tener que realizar un gran esfuerzo tanto a emisores como a receptores de mensajes cifrados con dicho método.

Durante algo más de doscientos cincuenta años, la Cifra Vigenère fue considerada prácticamente impenetrable, sin embargo la aparición en escena en la primera mitad del siglo XIX de la excéntrica figura del inglés Charles Babbage (1791-1871) como el principal protagonista del criptoanálisis de la época supuso un punto de inflexión. Babbage, entre otras cosas, es considerado como uno de los precursores de la que hoy consideramos una de las herramientas cotidianas más importantes como es el ordenador. Babbage se interesó por la desencriptación desde que era muy joven. En una ocasión, recordó cómo esa afición de su infancia le había proporcionado en ocasiones más de un quebradero de cabeza:

> *"Los chicos mayores hacían cifras, pero si yo conseguía unas pocas palabras, generalmente descubría la clave. En ocasiones, la consecuencia de este ingenio resultó dolorosa: los dueños de las cifras detectadas a veces me daban una paliza, a pesar de que la culpa la tenía su propia estupidez."*

Estas palizas no le desanimaron, al contrario, sirvieron de acicate para continuar cautivado por el criptoanálisis. En su autobiografía escribió *"... descifrar es, en mi opinión, una de las artes más fascinantes"*.

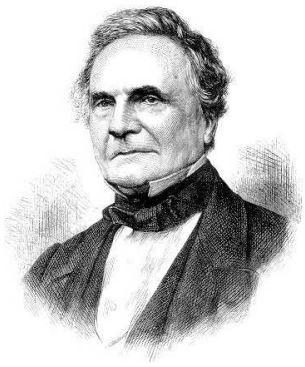

Figura 5. Charles Babbage.[5]

El interés de Babbage por la Cifra Vigenère se había producido en cierto modo de una manera fortuita, gracias a la intervención de un dentista de Bristol aficionado a la criptografía llamado John Hall Brock Thwaites. Resulta que en 1854, Thwaites afirmó haber inventado una nueva cifra, que en su desconocimiento de la Cifra Vigenère, resultaba similar a ésta, y escribió sobre sus avances en el *Journal of Society of Arts*, con la firme intención de patentar su descubrimiento. Babbage escribió a esa sociedad poniendo de manifiesto que Thwaites llegaba con varios siglos de retraso manifestando *"la cifra ... es muy antigua, y aparece en multitud de libros"*. En lugar de retractarse Thwaites adoptó una posición desafiante y no pidió ningún tipo de disculpas instando a Babbage a que aceptara el reto de descifrar una de las cifras generadas con su idea. Descifrable o no, no tenía relación alguna con el hecho de que fuera o no nueva, pero este nuevo reto despertó la curiosidad de Babbage que se embarcó en la búsqueda de un punto débil en la Cifra Vigenère.

¿Pero cómo fue capaz Babbage de desencriptar una cifra supuestamente indescifrable? Pongamos un ejemplo para comprender el proceso. Imaginemos que nuestra palabra clave es "SUR", y que el mensaje que queremos encriptar es "El adulto y el joven en el espejo". Nuestro mensaje se encriptaría haciendo uso de los alfabetos cifrados 18, 20 y 17, repitiendo este ciclo hasta concluir el mensaje. En la Tabla 4 podemos observar que los tres determinantes "el" del texto

[5] http://es.wikipedia.org/wiki/Charles_Babbage

Tabla 4. Encriptación de mensaje mediante el Cifrado de Vigenère (II).

Texto Llano Orig.	E l a d u l t o y e l j o v e n e n e l e s p e j o
Clave	S U R S U R S U R S U R S U R S U R S U R S U R S U
Texto Cifrado	W F R V O C L I P W F A G P V F Y E W F V K J V B I

llano original, se repiten en el mensaje cifrado. Esto es porque sus letras ocupan las posiciones 1-2, 10-11 y 19-20, es decir cada determinante está separado 9 posiciones del otro, que resulta múltiplo de la palabra clave "SUR" que es de 3 letras. Estas repeticiones no pasaron desapercibidas para Babbage y le proporcionaron un punto de partida desde el que comenzar a romper la Cifra Vigenère.

La brillante técnica empleada por Babbage consistía en una especie de estudio de frecuencias pero adaptada a la particularidad de la Cifra Vigenère. Imaginemos que se ha interceptado el mensaje de la Tabla 5, del cual únicamente se sabe que ha sido encriptado con la Cifra Vigenère, pero del que se desconoce la palabra clave utilizada.

La primera fase del ataque al código llevada a cabo por Babbage, consistió en buscar secuencias de letras que aparecieran más de una vez en el texto, esto es buscar patrones de repetición de caracteres, y una vez encontrado alguno ver la distancia de separación entre uno y otro para ver la multiplicidad de dicha distancia y de este modo establecer una hipótesis sobre la longitud de la palabra clave.

Tabla 5. Texto cifrado interceptado con patrones de repetición resaltados.

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

Analizando el texto cifrado, se procedería a construir una tabla de observación de patrones de repetición de caracteres, y la separación entre ellos, donde se representa la multiplicidad de esta separación (Tabla 6).

Aunque todavía no se tenga demasiada información sobre el mensaje cifrado, tras enumerar qué secuencias se repiten, así como los espacios que hay entre las repeticiones, el resto de la Tabla 6 trata de identificar los factores de los espaciamientos: la división entera de estos espaciamientos. Por ejemplo, la secuencia HISIEKA se repite tras 112 letras, por lo que los números

Tabla 6. Patrones de repetición de caracteres y espaciado entre ellos.

			Posible longitud de la clave (o factores)																	
Secuencia	Repetición	Separación	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
HISIEKA	2	112	✓		✓			✓	✓						✓		✓				
TIQ	5	21		✓				✓													
		35				✓		✓													
		329						✓													
		364	✓		✓			✓						✓	✓						
		385				✓		✓				✓									
		399		✓				✓												✓	
		420	✓	✓	✓	✓	✓	✓			✓		✓		✓	✓					✓
		728	✓		✓			✓	✓		✓			✓	✓						
		749						✓													
DRG	2	329						✓													
VOXSE	2	266	✓					✓							✓					✓	

2, 4, 7, 8, 14 y 16 son factores, ya que pueden dividir exactamente a 112 sin dejar decimales. Parece lógico considerar que la palabra clave tiene una longitud de 7 caracteres, ya que este factor se repite en todas las secuencias. En principio no conocemos aún la palabra clave con la que el mensaje ha sido cifrado, por lo que consideraremos que se trata de la palabra X1-X2-X3-X4-X5-X6-X7. Cada una de estas letras proporciona un alfabeto de cifrado, de forma que el cifrado polialfabético puede ser considerado como una combinación de 7 cifrados monoalfabéticos responsables cada uno de ellos de un séptimo de la codificación del total del mensaje. Luego las letras 1^a, 8^a, 15^a, 22^a, ..., estarán codificadas por el alfabeto cifrado correspondiente a X1. Parece evidente que conocer la palabra clave tanto para el emisor como para el receptor es una fase crucial en el desencriptado del texto llano original. Llegado a este punto podemos recurrir al análisis de frecuencias monoalfabético ya visto anteriormente. Para ello se lleva a cabo en el texto cifrado un "conteo" de las frecuencias de aparición de cada uno de los caracteres del alfabeto correspondiente al carácter X1 (Figura 6).

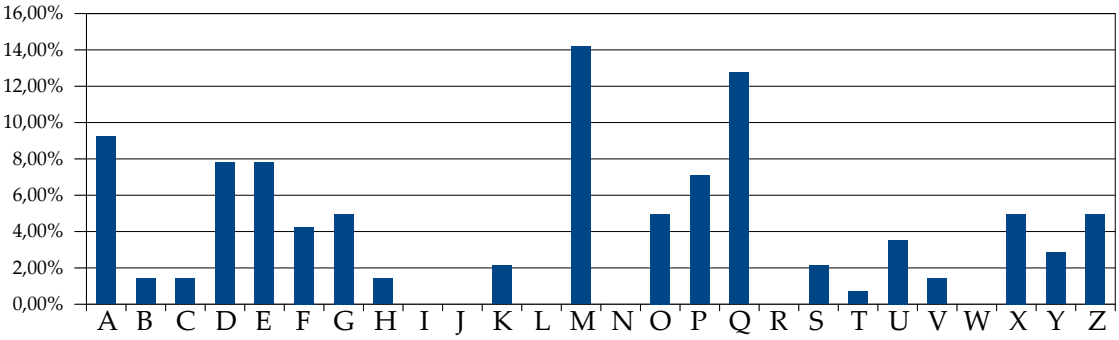

Figura 6. Distribución de frecuencias para las letras del texto cifrado, codificado utilizando el alfabeto cifrado X1 (porcentaje de apariciones).

En este punto ha de recordarse que cada alfabeto cifrado del cuadro Vigenère es simplemente un alfabeto normal desplazado entre 1 y 26 posiciones. Por esta razón, la distribución de frecuencias de la Figura 6 debería tener rasgos similares a la distribución de frecuencias de un alfabeto normal, excepto que habrá sido desplazado unas cuantas posiciones.

Si se realiza una comparativa gráfica de las Figuras 6 y 7, ambas debieran superponerse aunque con un desplazamiento, ya que recordemos que los alfabetos cifrados de la Tábula de Vigenère son generados por el desplazamiento de varios caracteres con respecto al alfabeto

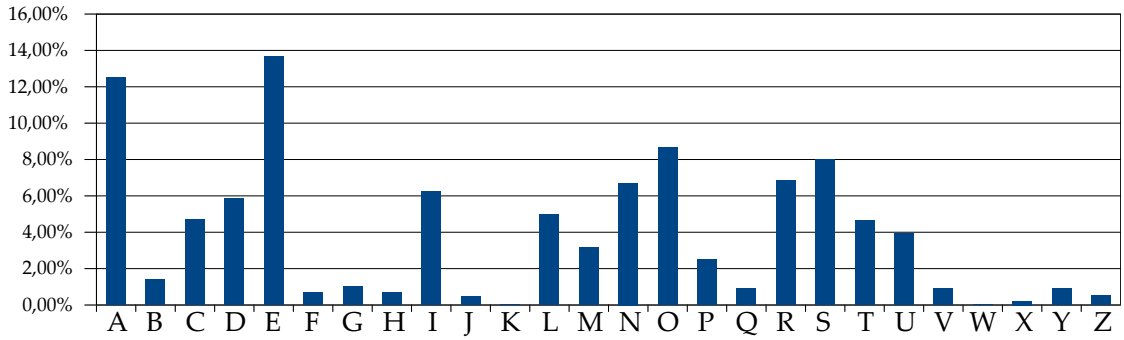

Figura 7. Distribución de frecuencias de caracteres para el idioma castellano.

llano original. Fijándonos en los patrones más representativos podemos ver que los bloques "MNOPQ", "XYZA" y "DEFGH" del alfabeto cifrado, se corresponden respectivamente con los bloques "ABCDE", "LMNO" y "RSTUV" del alfabeto llano. De este modo podemos considerar que el alfabeto llano se corresponde con el alfabeto cifrado identificado por la letra "M", es decir el número 12.

Identificado este primer alfabeto, procederíamos del mismo modo con el resto de caracteres de la palabra clave, esto es X2, X3, . . . , actividad que proponemos al lector como juego de entrenamiento. Llegaríamos a la conclusión de que el texto cifrado interceptado puede encriptarse-desencriptarse con la palabra clave "MERCADO". Descubierta la palabra clave el resto es una tarea relativamente sencilla.

Tabla 7. Texto original desencriptado (de la novela de Alejandro Dumas "El Conde de Montecristo").

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

Es muy probable que la técnica de criptoanálisis de la cifra Vigenère utilizada por Babbage se realizara en torno a 1854, poco después de su altercado con Thwaites, sin embargo su descubrimiento no tuvo ningún tipo de repercusión ya que nunca publicó sus logros. El descubrimiento

no se conoció hasta 1920, cuando gran parte de los trabajos de Babbage fueron examinados por un grupo de investigadores. De forma paralela pero independiente, el oficial retirado del ejército prusiano Friedrich Wilhelm Kasiski (1805-1881) desarrolló una técnica criptográfica similar a la de Babbage, que publicó en 1863 en *"Die Geheimschriften und die Dechijfrirkunst"* (*"La escritura secreta y el arte del desciframiento"*), y que hoy día es conocida como la *Prueba Kasiski*. Según algunos historiadores, es posible que Babbage, aparte de que tenía el hábito de no finalizar la mayoría de proyectos en los que se embarcaba, no publicara sus descubrimientos debido a presiones recibidas por parte de la inteligencia británica, ya que la guerra de Crimea había estallado recientemente, lo que hace muy probable que los británicos quisieran gozar de una ventaja sobre sus enemigos rusos, obligando a Babbage a mantener su secreto.

2. Las máquinas de cifrado y Enigma

2.1. 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 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 todas fueron crackeadas por el enemigo. 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.

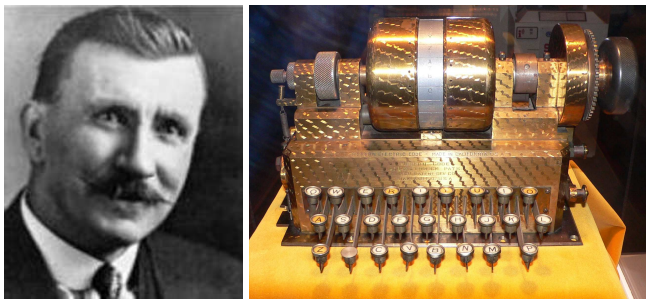

Figura 8. Edward Hugh Hebern (izq.) y Máquina Hebern (drcha.).[6]

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.

[6] http://ciphermachines.com/types.html
[7] http://dactilografo.blogspot.com.es/2011/02/me-guarda-un-secreto-el-funcionamiento.html

Figura 9. Arthur Scherbius.[7]

La segunda máquina de cifrado de rotores fue inventada en 1918. Ese año el ingeniero alemán Arthur Scherbius (1878-1929) 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 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.

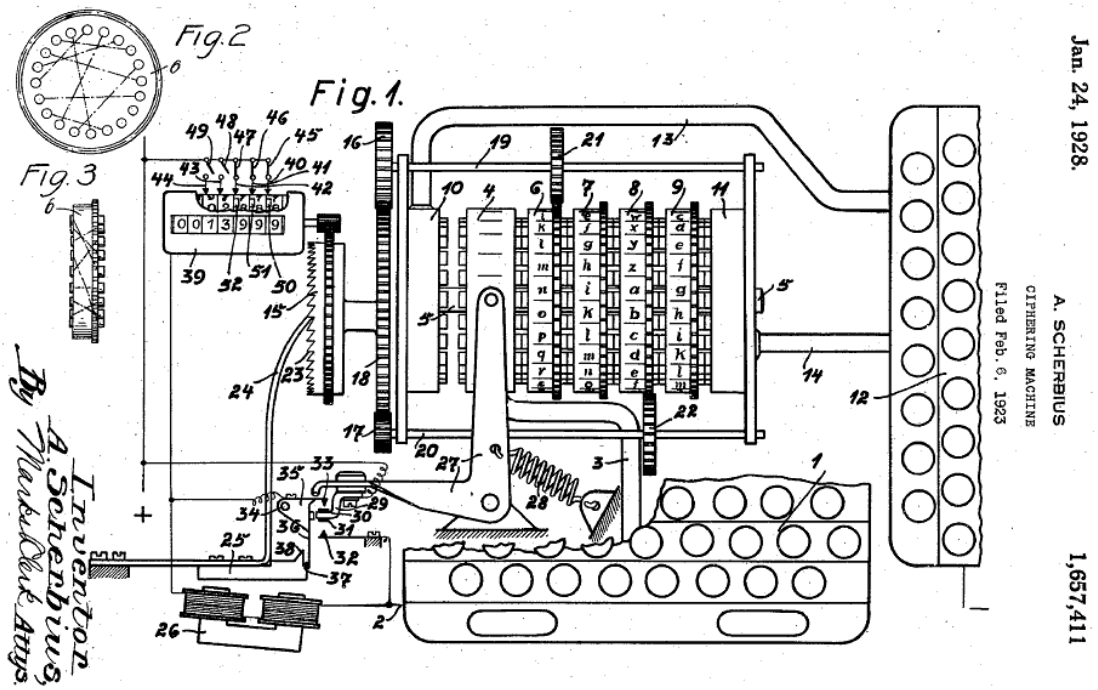

Figura 10. Patente americana (US - 1.657.411) de Enigma (A. Scherbius, 24 Enero - 1928).[8]

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

[8] http://en.wikipedia.org/wiki/Arthur_Scherbius

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 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 (*Kriegmarine*) 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.

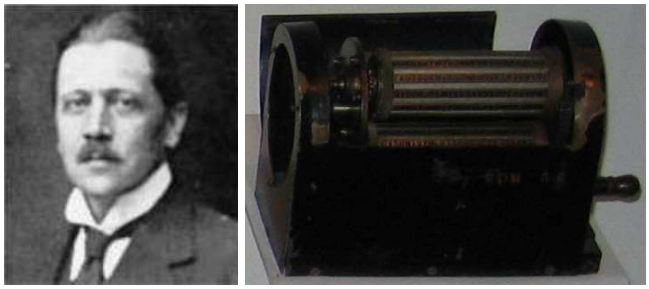

Figura 11. Arvid Gerhard Damm (izq.) y Prototipo Damm (drcha.).[9]

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). El hijo de Hagelin, Boris, que se habíia 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.

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

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

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.

2.2. El funcionamiento de Enigma

Enigma era muy similar a una máquina de escribir, salvo porque 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[10] con 6 pares de conexiones cableadas que podían conmutarse[11], un panel luminoso con 26 caracteres, varios rotores o modificadores (dependiendo de la versión de la Enigma), cada uno de los cuales contenía 26 ranuras dentadas 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 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 (que dependía de donde se situaba su muesca) 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, con la salvedad de que éstos dos últimos además de la rotación ya descrita, rotaban también cuando llegaban hasta la posición de su propia muesca. 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.

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.

2.3. 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:

[10] Abreviatura de *Steckerbrett* que en alemán significa "panel de conexiones de clavija". La versión comercial de Enigma no estaba dotada con este dispositivo que fue incluído en la versión militar con la intención de aumentar la seguridad.

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

[12] 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

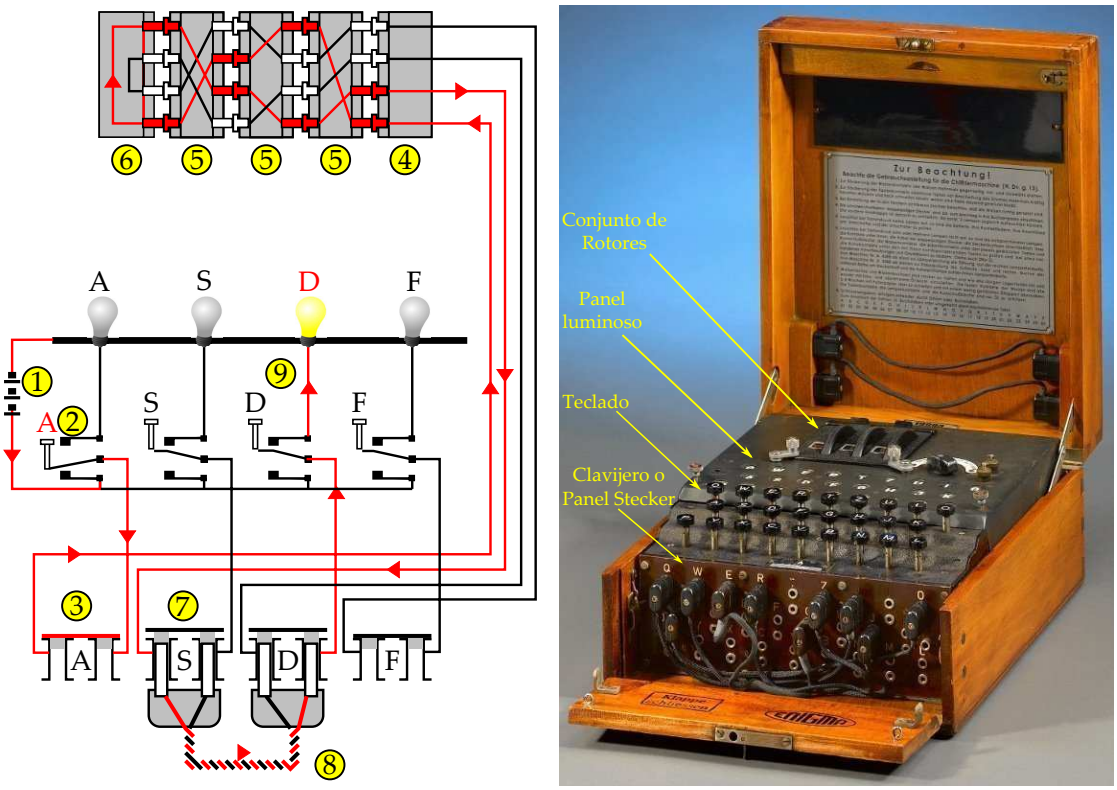

Figura 12. Diagrama de funcionamiento de Enigma y partes de la misma.[12]

- ✓ 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 (*"tageschlüssel"* en alemán) a utilizar en dicho mes[13], de modo que un operador podía leer en el libro algo así como:

- Walzenlage: II-III-I.
- Ringstellung: H-J-R.
- Grundstellung: Y-B-J.
- Stecker: 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

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

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.

Figura 13. 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 (los rotores de la 1ª 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 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.[14]

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" (en alemán *"spruchschlüssel"*). 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 cambios, y entonces procedía a codificar el mensaje a enviar. De este modo el mensaje transmitido comenzaba ZBH, que era la

[14] http://www.cryptomuseum.com/crypto/enigma/m4/index.htm y http://naukas.com/2012/12/24/.

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 ofrecía 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 en teoría inexpugnable, 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 sea necesario recurrir a notas escritas.
- ✓ Los criptogramas deberán mostrar resultados alfanuméricos.
- ✓ El sistema debe ser operable por una única persona.
- ✓ El sistema debe resultar fácilmente utilizable.

.

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

3.1. 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 Gwido Langer (1894-1948), y el mayor Maksymilian Ciężki (1894-1948) 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 (1900-1944), 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.

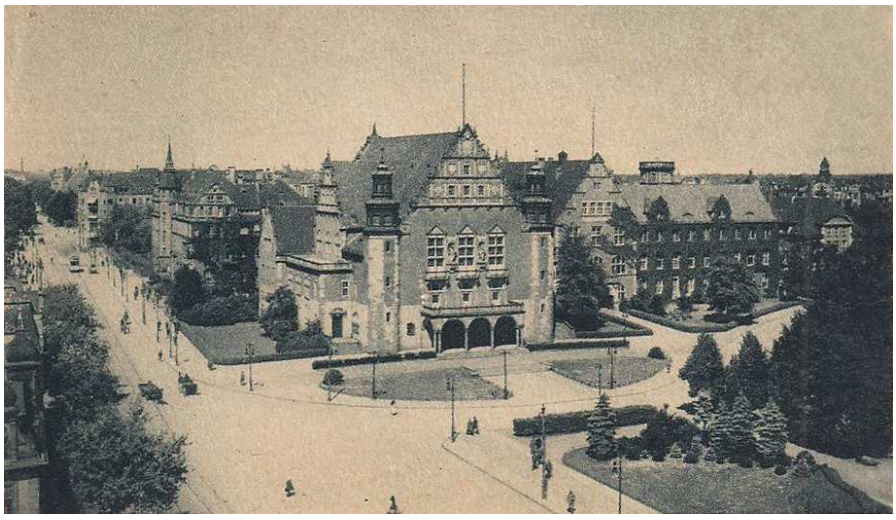

Figura 14. Universidad de Poznań (1929).

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 (1905-1980), Jerzy Różycki (1909-1942) y Henryk Zygalski (1908-1978), 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 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.

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
R	E	P	L	E	G
A	R	T	R	O	P
A	S	E	N	T	O
R	N	O	A	L	A
P	O	S	I	C	I
O	N	I	N	I	C
I	A	L			

$\Rightarrow$

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

$\Rightarrow$

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

$\Rightarrow$

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

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.

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 Ròżycki y Zygalski un poco después, comenzaron a trabajar como empleados del Biuro Szyfrów en Varsovia. Nacía así el BS4 y co-

menzaba la guerra contra Enigma.

3.2. 2ª Etapa. La aparición de *Asché*

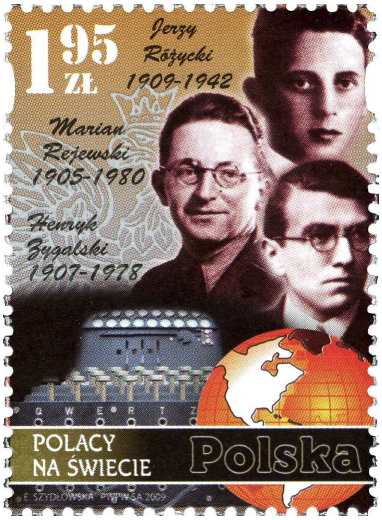

Figura 15. Miembros del BS4.[15]

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 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. 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

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

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 (1896-1976) 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.

Figura 16. Hans Thilo Schmidt.[16]

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 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.

Figura 17. Karol Gwido Langer.[17]

3.3. El Método de las Permutaciones. Fundamentación Teórica

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

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

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"[18]. 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:

$$P = (acb)(dfe)$$

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 Figura 12). 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.

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

Teoría de Permutaciones

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, decimos que una *permutación* de X es una aplicación biyectiva $\alpha : X \to X$. 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*.

Teoría de Permutaciones (cont.)

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

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

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

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 fijo a todos los elementos de $\{1,2,\ldots,n\}$ distintos de los s_i.

Con la finalidad de expresar la permutación anterior, se usa 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.*

Veamos un ejemplo. Consideremos las permutaciones expresadas en su notación cíclica $\sigma = (bf)(ac)(deg)$ y $\theta = (af)(bd)(ceh)$ de S_8. Como vemos ambas poseen una estructura cíclica idéntica. Para definir φ basta poner ambas permutaciones una encima de otra, obteniendo ("h" no aparece en σ, ni "g" en θ, por lo que $\varphi(h) = g$):

$$\begin{matrix} \sigma = (bf)(ac)(deg) \\ \theta = (af)(bd)(ceh) \end{matrix} \Rightarrow \varphi = \begin{pmatrix} a & b & c & d & e & f & g & h \\ b & a & d & c & e & f & h & g \end{pmatrix} \Rightarrow \varphi\sigma\varphi^{-1} = \theta$$

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 cuando va de izquierda a derecha. 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 8.

Tabla 8. Permutación total producida.

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	$SHNMLRL^{-1}M^{-1}N^{-1}H^{-1}S^{-1}$

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 global 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. 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:

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

De esta manera, como la permutación global de Enigma debe ser del mismo tipo que la provocada por el reflector ya que son conjugadas (ver pág. 82), dicha permutación global puede descomponerse siempre en el 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:

$$A = SHPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}H^{-1}S^{-1} = (SHPNP^{-1}ML)\,R\,(SHPNP^{-1}ML)^{-1} \quad (1)$$

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:

$$B = SHP^2NP^{-2}MLRL^{-1}M^{-1}P^2N^{-1}P^{-2}H^{-1}S^{-1} = (SHP^2NP^{-2}ML)\,R\,(SHP^2NP^{-2}ML)^{-1} \quad (2)$$

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

$$C = SHP^3NP^{-3}MLRL^{-1}M^{-1}P^3N^{-1}P^{-3}H^{-1}S^{-1} = (SHP^3NP^{-3}ML)\,R\,(SHP^3NP^{-3}ML)^{-1} \quad (3)$$

$$D = SHP^4NP^{-4}MLRL^{-1}M^{-1}P^4N^{-1}P^{-4}H^{-1}S^{-1} = (SHP^4NP^{-4}ML)\,R\,(SHP^4NP^{-4}ML)^{-1} \quad (4)$$

$$E = SHP^5NP^{-5}MLRL^{-1}M^{-1}P^5N^{-1}P^{-5}H^{-1}S^{-1} = (SHP^5NP^{-5}ML)\,R\,(SHP^5NP^{-5}ML)^{-1} \quad (5)$$

$$F = SHP^6NP^{-6}MLRL^{-1}M^{-1}P^6N^{-1}P^{-6}H^{-1}S^{-1} = (SHP^6NP^{-6}ML)\,R\,(SHP^6NP^{-6}ML)^{-1} \quad (6)$$

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 representaban la configuración inicial de partida de los rotores. Imaginemos que "sol" es dicha clave maestra. A continuación el operador elegía una "clave de sesión"[19] 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.

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:

$$A(x) = b;\ D(x) = r$$

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":

$$AD(b) = r$$

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:

[19] También llamada clave del mensaje.

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" $\to$ "a", "e" $\to$ "w", "n" $\to$ "v", "r" $\to$ "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:

$$AD = (aioukfcqxnvsg)(brdjzpewmthyl)^{20}$$

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:

$$A = SHPNP^{-1}QPN^{-1}P^{-1}H^{-1}S^{-1}$$

$$B = SHP^2NP^{-2}QP^2N^{-1}P^{-2}H^{-1}S^{-1}$$

$$C = SHP^3NP^{-3}QP^3N^{-1}P^{-3}H^{-1}S^{-1}$$

$$D = SHP^4NP^{-4}QP^4N^{-1}P^{-4}H^{-1}S^{-1}$$

$$E = SHP^5NP^{-5}QP^5N^{-1}P^{-5}H^{-1}S^{-1}$$

$$F = SHP^6NP^{-6}QP^6N^{-1}P^{-6}H^{-1}S^{-1}$$

$$AD = SHPNP^{-1}QPN^{-1}P^3NP^{-4}QP^4N^{-1}P^{-4}H^{-1}S^{-1}$$

$$BE = SHP^2NP^{-2}QP^2N^{-1}P^3NP^{-5}QP^5N^{-1}P^{-5}H^{-1}S^{-1}$$

$$CF = SHP^3NP^{-3}QP^3N^{-1}P^3NP^{-6}QP^6N^{-1}P^{-6}H^{-1}S^{-1}$$

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.

[20] 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*.

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:

Si $X = (a_1\, a_2)\,(a_3\, a_4)\,(a_5\, a_6)\,\ldots\,(a_{2k-3}\, a_{2k-2})\,(a_{2k-1}\, a_{2k})$,

e $Y = (a_2\, a_3)\,(a_4\, a_5)\,(a_6\, a_7)\,\ldots\,(a_{2k-2}\, a_{2k-1})\,(a_{2k}\, a_1)$,

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 [5, 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,* $K = (\ldots\, i\, j\,\ldots)$*; entonces* $T^{-1}KT = (\ldots\, T(i)\, T(j)\,\ldots)$ *Nótese que esto implica que* $K = (\ldots\, i\, j\,\ldots)$ *y* $T^{-1}KT = (\ldots\, T(i)\, T(j)\,\ldots)$ *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:

$$H^{-1}S^{-1}ASH = PNP^{-1}QPN^{-1}P^{-1}$$

$$H^{-1}S^{-1}BSH = P^{2}NP^{-2}QP^{2}N^{-1}P^{-2}$$

$$H^{-1}S^{-1}CSH = P^{3}NP^{-3}QP^{3}N^{-1}P^{-3}$$

$$H^{-1}S^{-1}DSH = P^{4}NP^{-4}QP^{4}N^{-1}P^{-4}$$

$$H^{-1}S^{-1}ESH = P^{5}NP^{-5}QP^{5}N^{-1}P^{-5}$$

$$H^{-1}S^{-1}FSH = P^{6}NP^{-6}QP^{6}N^{-1}P^{-6}$$

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

$$U = P^{-1}H^{-1}S^{-1}ASHP = NP^{-1}QPN^{-1}$$

$$V = P^{-1}H^{-1}S^{-1}BSHP = NP^{-2}QP^{2}N^{-1}$$

$$W = P^{-1}H^{-1}S^{-1}CSHP = NP^{-3}QP^{3}N^{-1}$$

$$X = P^{-1}H^{-1}S^{-1}DSHP = NP^{-4}QP^{4}N^{-1}$$

$$Y = P^{-1}H^{-1}S^{-1}ESHP = NP^{-5}QP^{5}N^{-1}$$

$$Z = P^{-1}H^{-1}S^{-1}FSHP = NP^{-6}QP^{6}N^{-1}$$

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

$$UV = NP^{-1}[QP^{-1}QP]PN^{-1}$$

$$VW = NP^{-2}[QP^{-1}QP]P^2N^{-1}$$

$$WX = NP^{-3}[QP^{-1}QP]P^3N^{-1}$$

$$XY = NP^{-4}[QP^{-1}QP]P^4N^{-1}$$

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

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 franceses y británicos en una reunión a las afueras de Varsovia de la que posteriormente hablaremos, la primera pregunta del reputado criptólogo británico Dillwyn Knox a Rejewski fue: "*¿cuál es la permutación del cilindro de entrada?*". Al escuchar la trivialidad de la respuesta, parece que Knox montó en cólera por no haber considerado una posibilidad tan obvia.

3.4. 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 [19, 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."*

Figura 18. Palacio Sajón en Varsovia (entre 1930 y 1935).[21]

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 Rejeski,

[21] 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 contra 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

consideraron oportuno reforzar las tareas criptológicas, por lo que la plantilla se aumentó a 6 operarios de descifrado, entre ellos Jerzy Ròżycki 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 de cada mensaje 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

El Ciclómetro

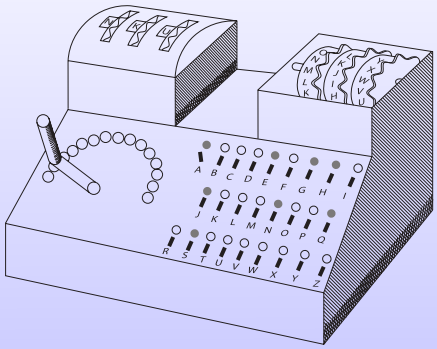

Figura 19. Diseño del Ciclómetro.

Con el fin de automatizar la tarea de confeccionar el catálogo de características, Rejewski y los polacos del BS4 construyeron el ciclómetro. La Figura 19 muestra una reproducción de dicho aparato realizada a partir de un diseño original del propio Rejewski. Este aparato estaba formado por dos bancos de rotores interconectados entre sí, de forma que el de la derecha iba desplazado tres posiciones con respecto al de la izquierda. Bajo dichos bancos de rotores estaban el panel de lámparas y las palancas, una por cada letra del alfabeto. Cuando una de estas palancas era accionada, una corriente eléctrica atravesaba varias veces ambos bancos de rotores y entonces se encendía un número par de lámparas, que eran las correspondientes a los dos ciclos asociados a la permutación AD. Entonces, accionando otra palanca de una letra no iluminada, se deducían dos ciclos asociados. De este modo se determinaba la descomposición en ciclos disjuntos de AD. Si se variaban entonces el orden de los rotores y sus posiciones iniciales, se calculaban todas las permutaciones AD existentes. Con todo esto, los polacos del BS4 elaboraban el catálogo, ya que las permutaciones BE y CF asociadas a una posición determinada de los rotores coincidían con la AD, sólo que bastaba adelantar los rotores de la derecha del ciclómetro una o dos posiciones respectivamente.

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, y que la configuración del Ringstellung se cambiaba todos los días.

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 2.3). 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 92:

$$\underline{\text{S}}\text{C GJVBJM} \Rightarrow \underline{\text{T}}\text{C GJVBJM} \qquad \text{ZD}\underline{\text{R}}\text{ WSXTGX} \Rightarrow \text{ZD}\underline{\text{T}}\text{ WSXTGX}$$

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 $\text{R} - \text{F} = \text{M}$, 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 $\text{M} - \text{F} = \text{H}$, 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 obtenía 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.

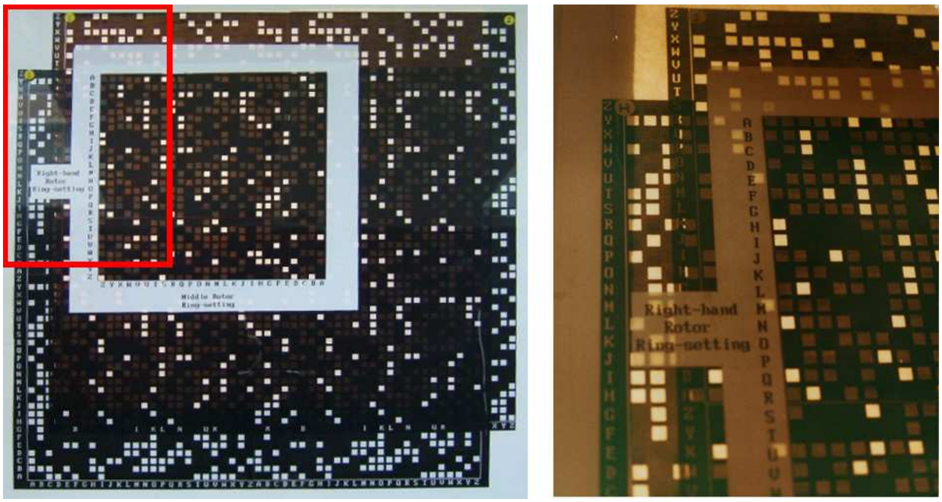

Figura 20. Hojas de Zygalski en el Museo de Bletchley Park.[22]

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 Tabla 9.

Tabla 9. Ejemplo de textos en alemán.

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 ...

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

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 Tabla 10.

Tabla 10. Textos cifrados con Enigma.

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 10 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 Ròżycki, 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.

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 represen-

taba 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.

Veamos un ejemplo de la operatividad de las bombas. A veces entre las females interceptadas, había tres de ellas que presentaban la repetición de una misma letra.

TGB FGTFAC VHJ DFMNFX ZGP FMSFNQ

La primera de estas females pone de manifiesto que el ciclo (F) se encuentra presente en la permutación AD. Imaginemos que la letra F no se viera alterada por el Stecker, es decir la F no está conectada a ninguna otra letra a través de una conexión de clavija. Entonces el ciclo (R) también aparece en la sustitución AD que se obtendría sin ninguna conexión en el Stecker. Tenemos ya conocimiento de que el número de tales productos AD es 105.456, tantos como posibles configuraciones de los rotores (orden y posiciones iniciales). De todos estos productos, desconocemos cuantos contienen al ciclo (F), sin embargo teniendo como aliado a la Teoría de Probabilidades, sabemos que fijado un ciclo de longitud 1, si A y D se eligen aleatoriamente entre las de su clase, entonces el 4 % de los productos AD contienen dicho ciclo, lo cual reduce drásticamente el anterior número de 105.456 en un factor de 0,04 cada vez que se observe una female con la letra F repetida. Como en nuestro ejemplo, $105.456 \cdot (0,04)^3 = 6,75$, existirán seis o siete configuraciones de rotores que ocasionen las tres females representadas en el ejemplo. Las máquinas ingeniadas por Rejewski eran las encargadas de automatizar la identificación de dichas configuraciones.

Desde el punto de vista de su diseño, la bomba consistía en tres ciclómetros conectados convenientemente. Un motor eléctrico permitía a los seis bancos de rotores girar de forma sincronizada recorriendo las 17.576 posiciones posibles. En el momento en el que se alcanzaba una posición en la que los tres ciclómetros reconocían el ciclo programado, (F) en el ejemplo expuesto, el mecanismo se detenía mostrando dicha posición.

Los polacos construyeron seis bombas, una por cada orden de los rotores. Previamente a su utilización, era preciso ajustar adecuadamente las posiciones de los rotores de los ciclómetros. Para ello, en primer lugar se normalizaban las females del mismo modo que se realizaba en las hojas de Zygalski. Entonces, se asociaba cada uno de los tres ciclómetros a una female y se colocaban sus rotores en la posición indicada en el Grundstellung, con el rotor derecho del segundo banco desplazado tres posiciones respecto a su homónimo del primer banco. En el ejemplo expuesto, el primer banco se colocaría en la posición "TGB", el segundo en la posición "TGE". Después de colocar los rotores se activaba la palanca de la letra F y el mecanismo de la bomba se accionaba. Las seis bombas encontraban las seis o siete posiciones que ocasionaban las tres females en unas dos horas. Entre esas posiciones se encontraba la que proporcionaba la clave, que para conocerla se seguía el mismo procedimiento que con los agujeros de las hojas de Zygalski.

Las bombas mecanizaron enormemente el proceso criptoanalítico, eliminando en gran parte los posibles errores debidos al factor humano. Sin embargo, su principal inconveniente era que se necesitaban al menos tres females con la misma letra repetida y que además dicha letra

permaneciera invariante por el Stecker, algo que no ocurría todos los días.

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.

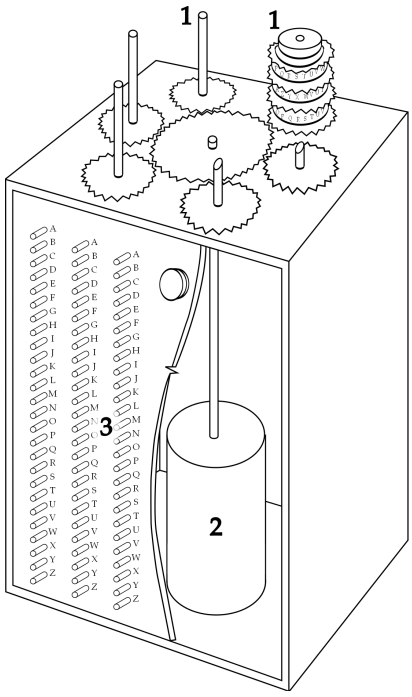

Figura 21. Bomba criptológica.[23]

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. Del mismo modo, ahora eran necesarias $26 \cdot 54 = 1404$ nuevas hojas de Zygalski. Además, el 1 de enero de 1939, los alemanes aumentaron el número de cableado del Stecker hasta 10, provocando un efecto devastador en las labores criptoanalíticas polacas. El método criptológico de Rejewski quedaba prácticamente anulado, de forma que tan sólo uno de cada diez días eran capaces de descifrar los mensajes alemanes. Sin embargo, los polacos contaron esta vez con la accidental "ayuda" del servicio de inteligencia del partido nazi para ser capaces de obtener el cableado interno de los nuevos rotores. Parece ser que la red de comunicaciones nazi incorporó los dos nuevos rotores, pero continuaba cifrando sus mensajes con el sistema previo al 15 de septiembre. Gracias a este desliz, pudieron obtenerse las conexiones de los nuevos rotores sin más que manipulando el antiguo sistema de ecuaciones fundamentado por Rejewski.

A pesar de obtener el cableado interno de los nuevos rotores, la capacidad de cálculo de la pequeña oficina polaca se veía completamente desbordada, y encima el 1 de enero de 1939 el método de las bombas de Rejewski quedaba totalmente inoperante ya que los alemanes incrementaron hasta diez el número de conexiones del Stecker. 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

[23] Diseño original de Rejewski. 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 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.

bomba. Enigma recuperaba virtualmente su inviolabilidad.

4. Bletchley Park

4.1. La herencia polaca

Figura 22. Puesto de radio a bordo de un Sd.KFz 251 del general de la 2ª División Panzer Heinz Guderian. Invasión de Francia (Mayo - 1940).[24]

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.

Bajo esta amenaza, los polacos decidieron que era necesario informar de sus avances criptoanalíticos, con el fin de que éstos no se perdieran. Si Polonia no podía beneficiarse del trabajo de Rejewski, al menos los aliados deberían tener la oportunidad de tratar de usarlos para seguir avanzando. Quizá Inglaterra o Francia, que contaban con más medios, fueran capaces de sacar el mayor partido al concepto de la bomba.

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 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

[24] Foto: Erich Borchert, Deutches Bundesarchive (Archivo Federal Alemán). Signatura: Bild+101I-769-0229-10A. http://www.bild.bundesarchiv.de/

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.

Figura 23. De izq. a drcha y de arriba a abajo: 1. Gustave Bertrand, 2. Alastair Denniston, 3. Maksymilian Ciężki, 4. Alfred Dillwyn Knox, 5. Wilfred Dunderdale y 6. Stewart Menzies.[25]

Durante años, los aliados habían considerado que Enigma era indescifrable, pero los logros conseguidos por los polacos puso de manifiesto la importancia de emplear a matemáticos en las técnicas de criptoanálisis. Bletchley Park, era la sede del Government Code & Cypher School (GC&CS, Escuela Gubernamental de Códigos y Cifras), una organización de descodificación recién fundada en Buckinghamshire, que tras el estallido de la guerra, se convirtió en la sede clandestina y secreta del ataque a Enigma. Bletchley Park era un edificio de arquitectura gótico Tudor, situado a las afueras de la pequeña localidad rural de Milton Keynes, sin duda un lugar insólito para uno de los mayores triunfos tecnológicos de la guerra.

Tras haber recibido la información sobre los logros del BS4, los criptólogos, científicos y matemáticos británicos de Bletchley dedicaron el otoño de 1939 a familiarizarse, comprender y dominar las técnicas polacas. A medida que los ingleses fueron asimilando conceptos y afinando esfuerzos, la actividad de Bletchley Park se fue incrementando más y más. De hecho al inicio de la guerra trabajaban en sus instalaciones en torno a 200 personas, pero al final de la misma esta cantidad aumentó hasta 10.000, lo que significó tener que realizar ampliaciones en el complejo, construyendo un gran número de cobertizos adicionales. Una vez pudieron entender y dominar las técnicas polacas, los criptoanalistas de Bletchley comenzaron a utilizar sus propios

[25] 1. [13], 2. http://enigma.umww.pl/index.php?page=Denniston, 3. http://wyborcza.pl/51,75248,5980398.html, 4. http://enigma.umww.pl/index.php?page=dillwyn-knox, 5. http://bondambitions.com/2011/01/origins-of-bond, 6. http://www.reformation.org/spies-are-despicable.html.

[26] http://es.wikipedia.org/wiki/Bletchley_Park

Figura 24. Fachada principal de Bletchley Park en la actualidad.[26]

atajos para descubrir las claves de la Enigma.

Figura 25. John R. F. Jeffreys.[27]

El primer método criptológico polaco utilizado por los británicos fue el de las hojas de Zygalski. A pesar de los cambios llevados a cabo por los alemanes en la operatividad de la Enigma, ahora los ingleses contaban con recursos humanos prácticamente ilimitados, por lo que este método era viable. La tarea de organizar todo el operativo le fue encargada a John R. F. Jeffreys (1918-1944), un matemático del Downing College de Cambridge reclutado por Alfred Dillwyn Knox junto a otros compañeros como Alan Turing, Goldon Welchman o Peter Twinn. Hacia finales de diciembre de 1939, los británicos tendrían preparadas las 1.560 hojas que eran necesarias. Dichas hojas eran una adaptación de las hojas de Zygalski, por lo que en Bletchley se las denominaron hojas de Jeffreys. Al mismo tiempo que se preparaban las hojas, un equipo se encargó de analizar el tráfico de mensajes, con el fin de identificar distintas redes de comunicaciones del ejército alemán, las emisoras que operaban dentro de cada red, aquella que gestionaba el tráfico dentro de la red, qué emisora transmitía cada mensaje y a cuál otra iba dirigido. Este análisis se convirtió en fundamental para descifrar los mensajes, ya que cada una de las redes funcionaba con una clave diferente.

El método de Zygalski necesitaba una gran cantidad de recursos, por lo que los británicos comenzaron a reclutar a una amplia variedad de personal, entre los que se encontraban matemáticos de Cambridge y sus alumnos de últimos cursos, ingenieros, lintgüistas, jugadores de ajedrez, secretarias, administrativos de apoyo … En total se estima que a lo largo de la guerra, unas 12.000 personas trabajaron en Bletchley Park de forma fija o temporal. Curiosamente un alto porcentaje de estas personas fueron mujeres.

Los británicos se percataron del hecho de que los operadores alemanes utilizaban claves relativamente obvias de descubrir. Para cada mensaje se suponía que el operador elegía una clave de mensaje diferente, tres letras escogidas al azar. Sin embargo, en el fragor de la batalla,

[27] http://enigma.wikispaces.com/John+Jeffreys

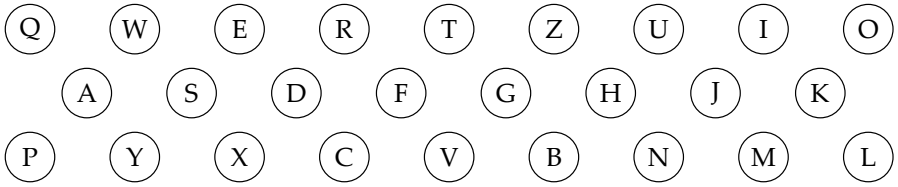

Figura 26. Disposición del teclado de la Enigma.

en vez de forzar su imaginación para elegir una clave al azar, los agotados operadores a veces tomaban tres letras consecutivas del teclado de la Enigma, como, por ejemplo, QWE o BNM. Este tipo de debilidades "de uso" más que fragilidad provocado por el propio diseño de la máquina, se denominaron *cillis*. Además de las cillis, existían otro tipo de errores humanos producidos por los propios responsables de la elaboración de los libros de códigos. La norma de prohibir que un mismo rotor permaneciera en el mismo hueco durante más de un día podría parecer una estrategia sensata, sin embargo, el efecto para el criptoanalista era que su trabajo se veía tremendamente simplificado por este hecho, ya que se reducía el número de posibles configuraciones de rotores que había que considerar para el estudio y análisis. Por supuesto, este hecho no pasó desapercibido a los criptoanalistas de Bletchley ya que descubrieron así una pequeña debilidad en la Enigma que no podían desaprovechar.

4.2. El genio de Turing

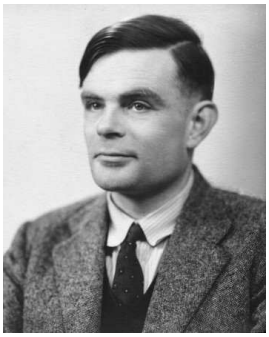

Figura 27. Alan Mathison Turing.[28]

El encargado de recoger el testigo de los logros criptográficos conseguidos por los polacos fue el genio matemático del King's College de Cambridge, Alan Turing (1912-1954). Turing ya había trabajado anteriormente en el desarrollo del concepto de máquina computacional. Son célebres sus trabajos de 1938 en los que define la *máquina-a* o *máquina de Turing*, una máquina virtual o física en el que era posible definir el concepto de *algoritmo* que resulta fundamental en computación. En Bletchley, Turing se convertiría en una de las cuatro figuras al mando de la organización de los trabajos de desencriptado junto a Gordon Welchman, Philip Stuart Milner-Barry y Conel Hugh O'Donel Alexander. Estaba al cargo del barracón 8, responsable de descifrar los códigos de la Enigma de la marina alemana (una de las más complicadas dado que contaba con un rotor adicional y sus operadores eran extremadamente escrupulosos a la hora de su utilización, lo que la hacía prácticamente impenetrable), con el fin de romper el bloqueo naval con el que los submarinos nazis tenían sometido al Reino Unido.

Parece ser que Turing se encargó personalmente de hacer llegar varios juegos de hojas de Jeffreys al equipo de criptólogos bajo el mando de Bertrand en Francia en enero de 1940. Debido a que los alemanes no tardarían en darse cuenta que su técnica de repetición de la clave del mensaje comprometía seriamente la seguridad de Enigma, el 10 de mayo de 1940, coincidiendo con la invasión de Francia, éstos modificaron nuevamente su sistema de cifrado, evitando la repetición de la clave de cada mensaje, hecho que resultó dramático para los aliados, puesto que de este modo se eliminaban así las females de las cabeceras de los mensajes y por lo tanto las hojas de Jeffreys quedaban inutilizables.

Turing se encargó de encontrar una manera alternativa de atacar la Enigma, una forma que no dependiera de la repetición de la clave del mensaje. Su técnica consistió en buscar lo que en

[28] Foto: Elliot&Fry (29 Mar. 1951), National Portrait Gallery (Galería Nacional de Retratos), Londres. http://www.npg.org.uk/collections/search/portrait/mw165875

criptología se denominan *puntales* (*cribs* en inglés) que no es otra cosa que cuando un fragmento de texto llano se puede asociar con un fragmento de texto cifrado. Después de unas pocas semanas estudiando mensajes cifrados interceptados, Turing podía adivinar (más bien predecir) partes de mensajes sabiendo sólo cuándo y desde dónde habían sido emitidos. Los alemanes tenían la costumbre de emitir mensajes cifrados a primera hora de la mañana, sobre las 6, en los que informaban del estado meteorológico a lo largo de todo el frente de guerra. Parecía razonablemente evidente que muchos de los mensajes interceptados en torno a las 6 de la mañana seguramente contendrían la palabra "wetter" (tiempo en alemán), lo cual suponía una fuente inmejorable para la obtención de puntales. Aunque en cierto modo eran suposiciones más que otra cosa, Turing estaba seguro de que por ahí podía desarrollar un método nuevo para atacar a Enigma. Pero considerar el ataque de un modo directo resultaba ser una tarea prácticamente inabordable. Por ello Turing adoptó una estrategia de ataque parecida a la de Rejewski, separando los efectos de las distintas configuraciones de los diferentes componentes de la máquina. Turing intentó separar por un lado el problema asociado a conocer la disposición de los rotores (en qué ranura estaban cada uno de ellos y cuáles eran sus orientaciones respectivas), y por otro el problema asociado al cableado utilizado en el clavijero o panel Stecker. De este modo si podía descubrir algo en un puntal que no tenía nada que ver con los cableados del clavijero, entonces no le resultaría imposible probar cada una de las restantes 1.054.560 combinaciones posibles de los rotores (60 disposiciones $\times$ 17.576 orientaciones). Si descubría las posiciones correctas de los rotores, entonces podía deducir las conexiones del Stecker. La diferencia sustancial con respecto a la estrategia de Rejewski es que Turing no estudió las repeticiones de las claves de los mensajes, sino la codificación de los puntales, que recordemos no dejaban de ser suposiciones. Si por ejemplo se estimaba que la palabra "wetter" era cifrada mediante el código ETJWPX, se estudiaban lo que se denominó *rizos internos*.

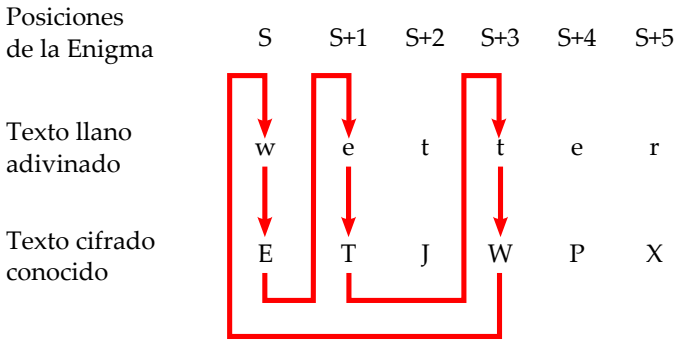

Figura 28. Rizos internos del puntal "wetter".

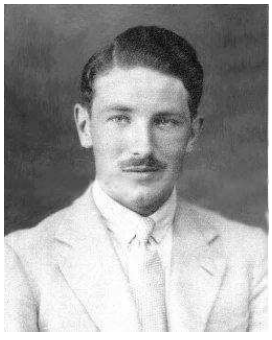

Figura 29. William Gordon Welchman.[29]

Como puede observarse en la Figura 28, en la posición S de la Enigma, la letra w es codificada como E, en la posición S+1, la e es codificada como T, y en la posición S+3, la t es codificada como W. Con la ayuda de los logros polacos, Turing fue capaz de construir un modelo mejorado de la bomba polaca, al que denominó *bombe* cuya finalidad consistía en ir probando multitud de posibilidades mediante la configuración inicial de los rizos establecidos por los puntales. La combinación de puntal, rizos y máquinas conectadas eléctricamente resultó ser finalmente una estrategia extraordinaria de criptoanálisis, capaz únicamente de ser planificada por una mente privilegiada como la de Turing. El primer modelo de *bombe*, denominado *Victory*, fue instalado en Bletchley en marzo de 1940 gracias a la obtención de 100.000 libras para la financiación del proyecto de Turing. Más tarde siguieron otros diseños mejorados por el también matemático Gordon Welch-

[29] http://www.specialforcesroh.com/image-4035.html

man (1906-1985), como el *Spider* en agosto de 1940, cuya principal implementación consistía en la inclusión del denominado *panel diagonal de Welchman* que tenía como función incrementar la efectividad de las máquinas diseñadas por Turing mediante el aprovechamiento de la reciprocidad de caracteres en el panel Stecker, de forma que si un caracter L_1 es permutado por otro L_2 mediante dicho panel, inevitablemente L_2 estará permutado por L_1 a través del Stecker. En la primavera de 1941 vería la luz el *Jumbo*. Las *bombe* eran capaces de identificar palabras en los textos cifrados con una gran probabilidad mediante la técnica denominada *crib*. Mecánicamente, los rotores de las bombe tenían el mismo cableado interno que la Enigma, y el reflector era simulado gracias a un sistema tan sencillo como que las conexiones y cables estaban presentes por duplicado. Para cada posible posición de los rotores se hacía una prueba, y si el resultado era una contradicción entonces esas posiciones de los rotores eran descartadas; en caso contrario, se seleccionaban esas posiciones como solución candidata.

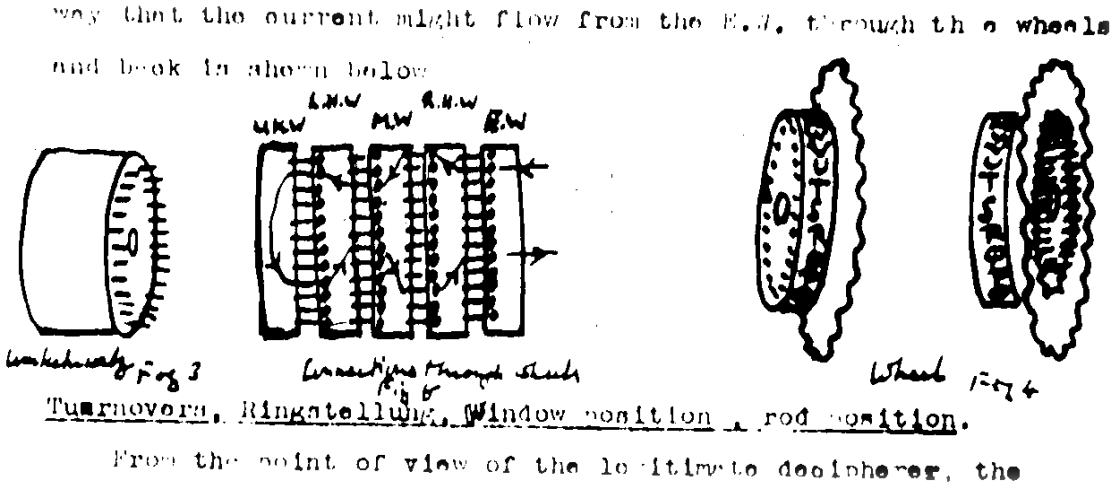

Figura 30. Notas del "Tratado sobre Enigma", manuscrito original de Alan Turing (1939-42).[30]

A finales de 1941, los alemanes sospecharon que los aliados habían conseguido desencriptar el código de la Enigma, por lo que añadieron un cuarto rotor, cuyo cableado interno era totalmente desconocido para los criptólogos de Bletchley. Sin embargo, en las navidades de ese mismo año sucedió un hecho inesperado. Uno de los submarinos emitió un mensaje, pero inexplicablemente el operador utilizó una Enigma de tres rotores, lo que ofreció a los aliados la posibilidad de poder establecer una reciprocidad entre los dos sistemas y deducir el cableado interno del cuarto rotor, y por lo tanto la posibilidad de seguir trabajando en la desencriptación del código. Aunque hubo un periodo de "apagón" que duró casi nueve meses, a finales de octubre de 1942 los criptoanalistas británicos lograron desentrañar el nuevo código.

Cuando la guerra llegaba a su fin, Bletchley Park estaba dotada con 211 máquinas *bombe*, que necesitaban mas de 2.000 personas para su mantenimiento y utilización. El trabajo de Alan Turing y sus *bombe* ayudaron enormemente a que los aliados ganaran la guerra. Hechos importantes que así lo demuestran son el papel que la desencriptación del código Enigma significó en la Batalla del Atlántico en la defensa de los convoyes navales aliados contra los submarinos alemanes, la derrota del Afrikakorps de Rommel, o el desembarco de Normandía. Con la victoria aliada, el primer ministro británico Wiston Churchill consideró oportuno que era necesario destruir todas las *bombe* y toda la documentación relacionada con su diseño y construcción, a pesar del valiosísimo servicio que habían proporcionado durante la guerra. Además todos los participantes en las labores de descodificación de Enigma tuvieron que prestar juramento de que en ningún caso revelarían dato alguno sobre las actividades llevadas a cabo en Bletchley Park du-

[30] http://www.turingarchive.org/browse.php/C/30

rante la contienda. A partir de 1976 la información sobre Enigma comenzó a ser desclasificada y dada a conocer al público en general, fue entonces cuando todos aquellos que colaboraron en la lucha contra Enigma y que tan injustamente habían sido tratados debido a las circunstancias de la guerra fría, comenzaron a gozar del reconocimiento público que merecían.

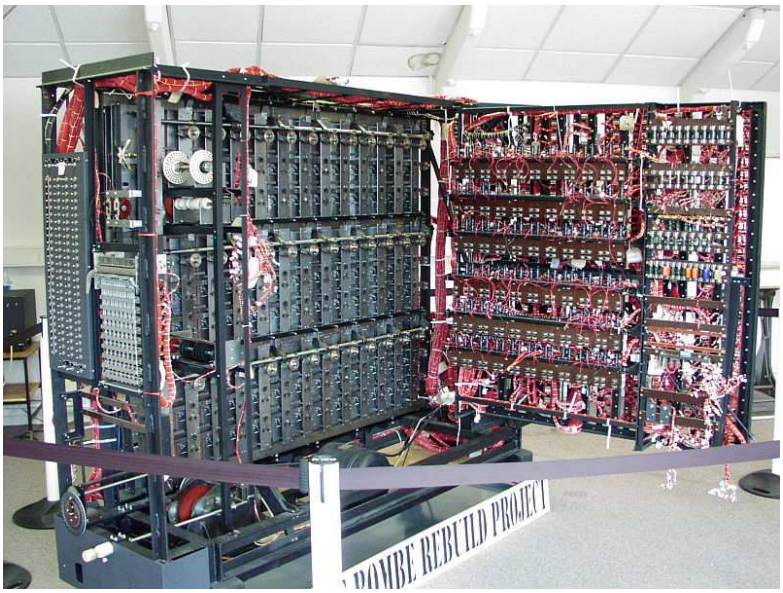

Figura 31. Réplica de la bombe, reconstruida gracias al trabajo de técnicos veteranos voluntarios de Bletchley Park.[31]

5. El final de los protagonistas de Enigma

Tras la invasión de Polonia por los nazis, una gran cantidad de miembros del BS4 fueron capturados, torturados y asesinados. Afortunadamente, Rejewski, Ròżycki 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"[32]. El centro se dedicó a interceptar transmisiones de radio alemanas en coordinación con el GC&CS británico. 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.

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

[31] http://en.wikipedia.org/wiki/File:Bombe-rebuild.jpg
[32] Es posible encontrar que algunos autores lo denominan "PC Bruno", donde PC significa "Puesto de Mando".

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 acuñaría 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.

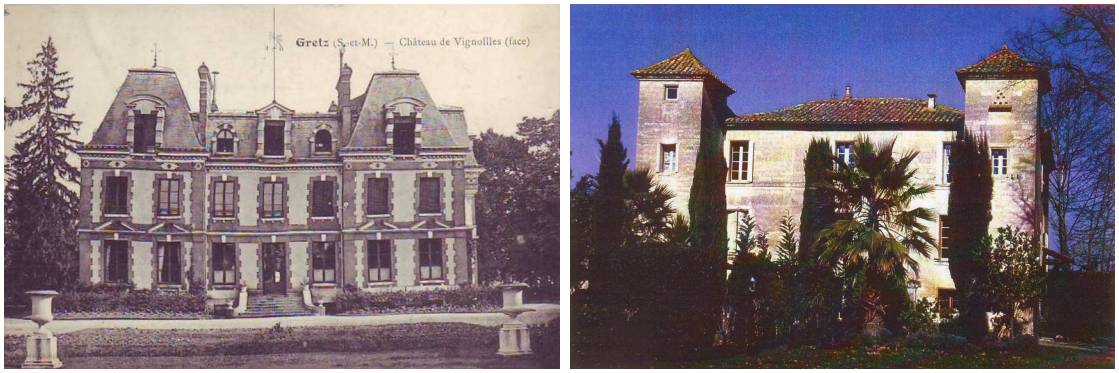

Figura 32. Château de Vignolles (izq.) y Château des Fouzes (drcha.) [13].

Figura 33. Trabajadores del centro polaco-hispano-francés de radioespionaje "Cadix" (1940-1942).[33]

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

[33] 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 Ròżycki. 20. Marian Rejewski. http://www.ww2.pl/ww2/zdjecia/153.jpg

[34] (a) De izq. a drcha.: 1. Henryk Zydalski, 2. Jercy Ròżycki, 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 Ròżycki; 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

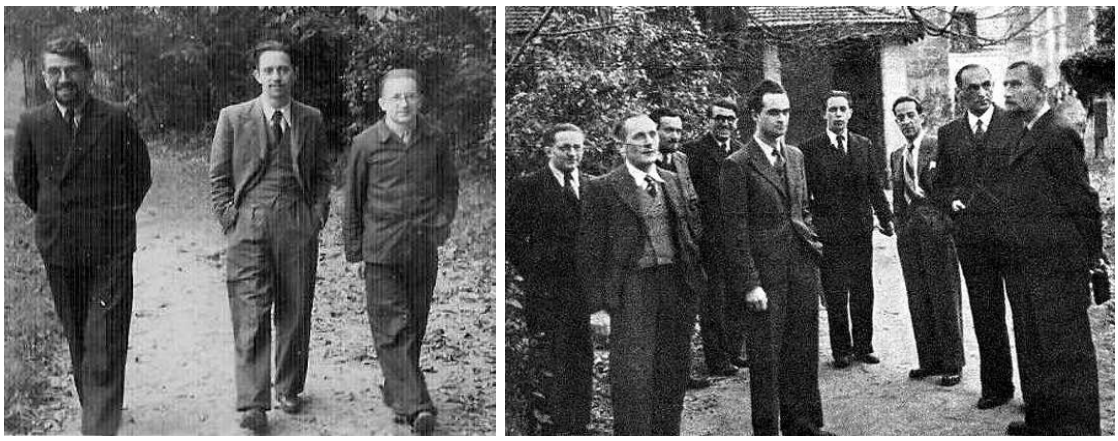

Figura 34. Imágenes en los jardines del Château des Fouzes en algún momento entre septiembre de 1940 y junio de 1941.[34]

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

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

Figura 35. De izqda. a drcha.: Jan Graliński, 2. Jercy Ròżycki, 3. Piotr Smolesński, en Cadix.[35]

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 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. 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

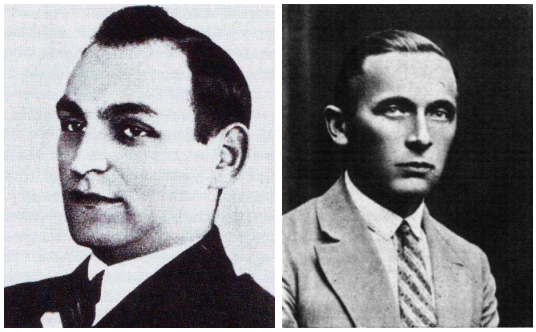

Figura 36. Antoni Palluth (izq.) y Edward Fokczyński (drcha.).[13]

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.

Figura 37. Estatua de bronce de Rejewski en Bydgoszcz, en conmemoración del centenario de su nacimiento (2005).[36]

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.

Resulta paradójico que la inestimable prestación que significaron los logros de Turing para los Aliados fueran recompensados de la manera en la que las instituciones británicas consideraron. En febrero de 1952, Turing dejó solo en su casa a su amante Arnold Murray. Al regresar, Turing se encontró con la sorpresa de que varios objetos de gran valor sentimental habían de-

[36] http://commons.wikimedia.org/wiki/File:Bydgoszcz_Rejewski_3.jpg?uselang=pl
[37] http://www.geograph.org.uk/photo/2261564

Figura 38. Monumento conmemorativo a los criptoanalistas polacos en Bletchley Park (2002).[37]

saparecido de su casa, por lo que se dispuso a denunciar dicho robo. En su declaración, Turing mencionó con total naturalidad su relación con Murray, por lo que la policía consideró oportuno investigar su homosexualidad en lugar del verdadero hecho trascendente que era el robo en sí mismo. En marzo de 1952, Turing era enviado a juicio, ya que en aquella época la conducta homosexual estaba penada por las autoridades británicas. Turing perdió el juicio aunque dado su prestigio, tuvo que someterse a un tratamiento de castración química mediante hormonas en lugar de su ingreso en prisión. Parece ser que este hecho provocó cambios fisiológicos en Turing que sufrió como su cuerpo cambiaba hasta el punto de experimentar el crecimiento de sus pechos. Harto de esta situación decidió quitarse la vida comiéndose una manzana a la que previamente había inyectado cianuro potásico.

Figura 39. Estatuas conmemorativas de Alan Turing en Bletchley Park (2008) y en Sackville Park, Manchester (2009).[38]

[38] http://es.wikipedia.org/wiki/Alan_Turing

En septiembre de 2009, el Primer Ministro Gordon Brown, solicitaba disculpas públicas por el trato que Turing había recibido, y manifestaba:

> *"Turing fue un destacado y brillante matemático, cuya labor más famosa fue descifrar los códigos Enigma del ejército alemán. No resulta exagerado señalar que, sin su extraordinaria contribución, la historia de la 2ª Guerra Mundial habría sido bien diferente. Él fue una de esas personas de las que verdaderamente podemos decir que contribuyó a modificar el rumbo de la guerra. La deuda de gratitud que tenemos con él hace mucho más horripilante que fuera tratado de forma tan inhumana.*
>
> *Miles de personas se han unido para solicitar justicia para Alan Turing y el reconocimiento del modo atroz en el que fue tratado . . . el trato que recibió fue completamente injusto, y me complace poder expresar lo consternado que me siento, que nos sentimos todos, por lo que ocurrió.*
>
> *. . . Más allá incluso, Alan merece reconocimiento por su contribución a la humanidad. Para aquellos de nosotros que nacimos después de 1945, en una Europa unida, democrática y en paz, es duro imaginar que nuestro continente fue una vez escenario del momento más oscuro de la humanidad.*
>
> *. . . Por lo tanto, en nombre del Gobierno británico, y de todos aquellos que vivimos en libertad gracias al trabajo de Alan, me siento orgulloso de decir: lo sentimos, mereciste algo mucho mejor."*

6. Las máquinas Lorenz

6.1. Características y particularidades

Muy a pesar del ingenio que supuso la ruptura del código de la Enigma, no fue ésta la máquina que inspiró el nacimiento de lo que hoy día podemos considerar (aunque con algunas restricciones) como el primer ordenador de la historia. Durante el curso de la 2ª Guerra Mundial, Alan Turing fue el encargado de romper el difícil código naval alemán (llamado *Shark*), lo que sirvió para que los aliados se hicieran finalmente con la victoria. Sin embargo, Enigma sólo significó la mitad de la historia de la lucha criptológica contra los alemanes.

En 1940, a principios de la guerra, los británicos interceptaron unas señales de teletipo en las que no se utilizaba el código Morse. Su "música" era completamente distinta al sonido característico proveniente de las Enigma. Se trataban de señales cifradas con las llamadas máquinas *Lorenz SZ40* y *SZ42* (*Schlüsselzusatz*, que significa "cifrado adjunto") que estaban conectadas a un teletipo. Mientras que la Enigma se usaba generalmente por unidades de combate, las Lorenz fueron utilizadas para las comunicaciones cifradas entre el propio Hitler y su alto mando. Esto es debido a que la cúpula del ejército nazi consideraban que las Lorenz ofrecían si cabe una mayor seguridad que las Enigma ya que utilizaban 12 rotores. En cierto modo las Lorenz sirvieron para "dictar" el curso

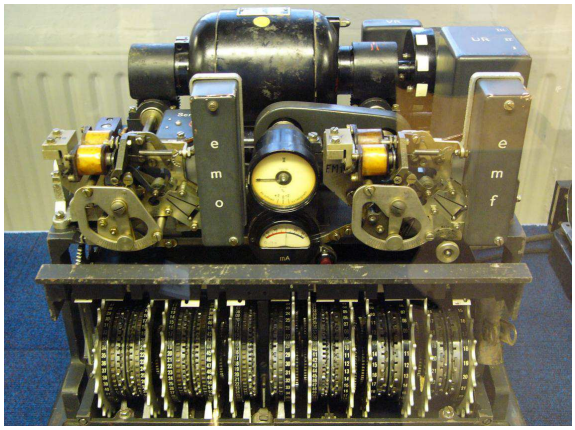

Figura 40. Máquina Lorenz SZ42.[39]

[39] http://es.wikipedia.org/wiki/Código_Lorenz

de la guerra. En Bletchley Park, los criptoanalistas organizaban su trabajo clasificándolo dependiendo de los códigos o claves con los que se referían a las distintas redes de comunicación utilizadas por los alemanes. El tráfico de las señales alemanas que circulaban a través de teletipo eran etiquetadas con la clave *Fish* (pez), y a su vez las que provenían de las máquinas Lorenz, se etiquetaron como *Tunny* (atún). La Figura 41 muestra las lineas de teletipo interceptadas y rotas por los aliados.

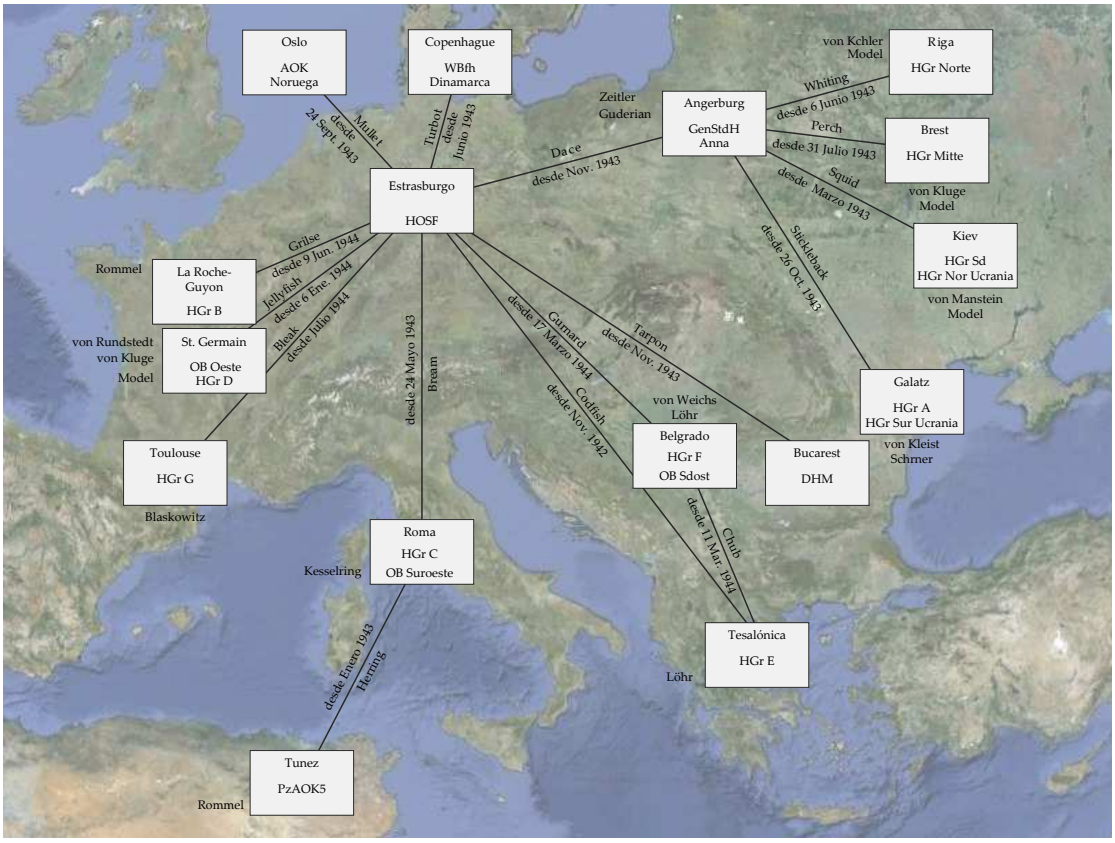

Figura 41. Líneas de teletipo interceptadas durante la 2ª Guerra Mundial. Los cuadros representan el destino de la línea de teletipo con el código de identificación alemán y el/los general/es al mando del destacamento nazi situado en ese destino. Se puede observar el nombre clave de las líneas como se conocían en Bletchley (todas con nombres de peces), y la fecha en la que se consiguió romper el código de encriptación por primera vez.

Figura 42. Equipos de operarios de Enigma.[40]

Si hiciéramos una comparativa con respecto a las Enigma, además de su mayor potencia de encriptación, las Lorenz tenían una ventaja muy clara con respecto a éstas. Mientras Enigma

[40] Imágenes cedidas por Helge Fykse (http://fykse.dnsalias.com/bilder/enigma/)

necesitaba en su operativa un mínimo de tres individuos tanto en el lugar de emisión como en el de recepción, esto es, un operador que tecleaba el mensaje con un ayudante que anotaba las letras a medida que éstas se encendían en la máquina, que finalmente proporcionaba a un operador de radio que emitía en código morse el mensaje cifrado. Del mismo modo se repetía un proceso similar pero al revés en el lugar de recepción del mensaje. Sin embargo, las Lorenz únicamente necesitaban un operador en el lugar de emisión y otro en el de recepción con el consiguiente ahorro de personal y por lo tanto un mayor aprovechamiento y optimización de los recursos humanos.

6.2. El algoritmo de codificación

Cada vez que se escribía un carácter desde el teclado éste era transformado mediante el Código Baudot[41]. Un carácter es representado por una secuencia de 5 bits, esto es, por una secuencia en binario compuesta de 5 dígitos, que en Bletchley Park se representaba mediante puntos y cruces (o 0 y 1 en binario). El método utilizado por la máquina Lorenz para encriptar un mensaje consistía en generar una secuencia aleatoria de 5 números binarios o bits y operar por parejas de bits, uno procedente de la letra a codificar y el otro de la secuencia aleatoria, de acuerdo con el operador booleano *XOR* al que también se conoce como *exclusivo OR*. La máquina en cuestión disponía de un total de 12 ruedas denominadas *pinwheels* con las que se generaba la secuencia aleatoria de 5 bits. De estas ruedas, cinco recibían el nombre de "chi" o χ y giraban paso a paso de modo regular, otras cinco llamadas "psi" o ψ giraban paso a paso de modo irregular, y finalmente había dos ruedas motoras, denominadas μ_1 y μ_2.

Imaginemos que se quiere codificar la letra M que en código Baudot resulta $\cdot\cdot\times\times\times$ (en binario: 00111) [23]. Los pasos a seguir son los siguientes:

1. El operador configura las ruedas χ con la posición inicial de los pines que equivalen a *off-on-on-off-on*, lo que significa que se invierten los valores de la codificación (puntos por cruces y cruces por puntos -en binario 0 por 1 y 1 por 0-) en aquellos dígitos correspondientes a la posición *on*. De esta manera $\cdot\cdot\times\times\times$ (00111) se convierte en $\cdot\times\cdot\times\cdot$ (01010).

2. En segunda instancia se aplica la suma aritmética en módulo 2 (similar a la aplicación del operador booleano *XOR*) a las parejas de bits procedentes de las secuencias que representan la letra M y la letra M modificada por las ruedas χ. Esta operación es de tal forma que si los dos bits son iguales el resultado es $\cdot$ (esto es $\times+\times=\cdot$, o bien $\cdot+\cdot=\cdot$), y si son distintos, el resultado es $\times$ (esto es $\times+\cdot=\times$, o bien $\cdot+\times=\times$)[42]. En este caso, tenemos

$$\cdot\cdot\times\times\times+\cdot\times\cdot\times\cdot=\cdot\times\times\cdot\times$$

   cuyo resultado es equivalente a 01101 en binario.

3. En tercer lugar el operador configura las ruedas ψ con la posición inicial de los pines que equivalen a *on-off-on-off-on* de modo que

$$\cdot\times\times\cdot\times\Rightarrow\times\times\cdot\cdot\cdot$$

[41] Un código inventado en 1874 parecido al ASCII de los ordenadores actuales, pero utilizado en telegrafía. El código original, conocido como Alfabeto Internacional de Telégrafía Número 1, dejó de utilizarse en 1901, ya que en su lugar apareció un código modificado por Donald Murray, donde se reordenaban algunos caracteres, propiciado por el desarrollo de un teclado parecido al de una máquina de escribir. Entonces la disposición de los bits fue disociada de las teclas del operador. Murray arregló su código de modo que los caracteres más usados produzcan la menor cantidad de cambios de estado, lo que reducía al mínimo el desgaste en el equipo. La Western Union desarrolló una nueva modificación del código de Murray. Esta modificación final supuso la supresión de algunos caracteres, y es la que se conoce generalmente como el Código Baudot, también conocido como Alfabeto Internacional de Telegrafía Nº2 (ITA2). El ITA2 todavía se utiliza en teléfonos para sordos, en radioaficionados, y en RTTY (radioteletipo).

[42] Esta operación "aritmética" fue inventada por un empleado de la división de desarrollo de la ATT llamado Gilbert S. Vernam, para permitir la aplicación intensiva en el teletipo del cifrado descrito durante la 1ª Guerra Mundial. Esta suma no era una suma convencional, sino la aplicación de una de las aritméticas binarias descritas por Boole, en particular la del operador *XOR*.

equivalente a 11000 en binario.

4. Por último se suman los dos últimos caracteres obtenidos, esto es

$$\cdot\times\times\cdot\times + \times\times\cdot\cdot\cdot = \cdot\times\cdot\times\cdot$$

equivalente a 01010 en binario, secuencia que en el código Baudot corresponde a la letra R, es decir resumiendo, la letra M se ha codificado como la letra R.

6.3. Criptoanálisis y desencriptado

La historia de la desencriptación del código de las máquinas Lorenz, resulta cuanto menos un tanto rocambolesca. Según parece el 30 de agosto de 1941, un operador alemán encargado de realizar comunicaciones a través de las Lorenz envió un mensaje cifrado de un tamaño bastante considerable, unos 4.000 caracteres tecleados directamente sin utilizar las tiras de papel, desde la ciudad de Atenas con destino Viena. El caso es que una vez enviado pacientemente el mensaje carácter a carácter, parece ser que el operador recibió otro de respuesta en alemán, solicitándole que por favor volviera a enviarlo de nuevo ya que no había sido recibido correctamente. Fue entonces cuando el operador cometió el error táctico de enviar nuevamente el mensaje con un idéntico indicador[43] (HQIBPEXEZMUG) de la máquina Lorenz a como lo había hecho la vez anterior, excepto que esta vez abrevió algunas de las palabras eliminando algunas letras de la terminación de las mismas. Este hecho constituyó un error gravísimo, ya que no respetó una de las normas básicas de la criptología, lo que puso de manifiesto una debilidad en las Lorenz, permitiendo que el equipo de criptoanalistas de Bletchley Park liderados por John Tiltman (1894-1982) comenzaran a analizar el código *Tunny*.

Tiltman, que gozaba de una reputada posición debido a sus trabajos contra las cifras militares japonesas, y algunas cifras alemanas entre otras, comenzó su análisis mediante una ingeniosa técnica. Si por ejemplo sumamos los caracteres J y P, obtenemos L; si a L le sumamos nuevamente P, obtenemos J, que era el carácter de partida.

Figura 43. John Hessel Tiltman.[44]

$$\times\times\cdot\times\cdot + \cdot\times\times\cdot\times = \times\cdot\times\times\times \Rightarrow \times\cdot\times\times\times + \cdot\times\times\cdot\times = \times\times\cdot\times\cdot$$

Una vez sumados los dos textos cifrados, obtuvo una cadena de caracteres que resultaba ser la suma de dos textos planos, esto es si tenemos P_1 y P_2, textos planos, y les sumamos la secuencia K para obtener los textos cifrados C_1 y C_2 ($P_i + K = C_i$, $i = 1, 2$), entonces al sumar los dos textos cifrados, obtendremos la suma de los dos textos planos, ya que en virtud de la propiedad anterior $C_1 + C_2 = (P_1 + K) + (P_2 + K)$, pero como hemos visto antes $K + K = 0$ (considerando por 0 el elemento neutro de esta aritmética). En este punto es necesario observar que si realizamos la suma de dos textos cifrados idénticamente iguales con la misma clave, el resultado es una secuencia de elementos neutros, por lo que los cambios pequeños introducidos por el operador del mensaje fueron lo suficientemente significativos para poder realizar el ataque criptológico. Una vez realizó la eliminación de la secuencia de cifrado, Tiltman sabía que cada carácter del texto resultante era la suma de otros dos que en el mensaje original distaban unas pocas posiciones. Comenzó entonces la tarea que

[43] Con anterioridad a octubre de 1942, los operadores alemanes, conforme al libro de códigos que les era entregado mensualmente, establecían en el preámbulo del mensaje cifrado con un código Tunny una secuencia de 12 caracteres que se denominaba *indicador*, relacionado directamente con la configuración inicial de cada una de las 12 ruedas de las Lorenz. En ocasiones escribían 12 nombres, por ejemplo Martha, Gustav, Otto, Ludwig, ..., que se correspondía con el indicador "MGOL ...". Si el emisor escribía el anterior indicador, el receptor sabía que la primera rueda ψ debía configurarse en la posición X de acuerdo al libro de códigos, siendo X la configuración de la letra M en el libro de códigos para el día de emisión del mensaje.

[44] http://www.rutherfordjournal.org/article030109.html

requería una mayor inspiración, que consistía en adivinar qué palabras combinadas (o sumadas) con el texto obtenido, podían revelar el mensaje original. Tiltman ya había demostrado sus cualidades "adivinatorias" en anteriores ocasiones, una habilidad adquirida y entrenada a lo largo de sus años de servicio. Uno de sus muchos logros, había consistido en la desencriptación de un mensaje cifrado mediante el código de Vernam en el verano de 1941. Un resultado directo de la estrategia seguida por Tiltman, tarea ésta que le había llevado 10 días, significaba que sumando el texto plano a cualquiera de los dos mensajes cifrados interceptados, se obtenía la secuencia de caracteres de la clave utilizada para cifrar los mensajes. Fue en ese instante cuando todo el equipo de Tiltman aunó esfuerzos con la esperanza de intentar hallar alguna lógica que explicara la aparente aleatoriedad de los caracteres obtenidos con las Lorenz.

Figura 44. William Thomas Tutte.[45]

¿Era posible que los alemanes hubieran inventado un sistema que generara secuencias aleatorias de manera sincronizada? Si fuera así, no cabría menor esperanza de éxito en la empresa en la que los británicos se acababan de enrolar. Por el contrario, mantenían el deseo de encontrar algún tipo de sistematización similar al que habían sido capaces de obtener con la Enigma. Sin embargo, el gran inconveniente con el que contaban era que nadie había llegado a ver nunca ninguna máquina similar, y la poca información que tenían sobre ella era muy pobre. Con este desamparado panorama, y tras muchos intentos infructuosos de descubrir algún tipo de sistematización que explicara aquella aparente aleatoriedad, en las navidades de 1941, Gerry Morgan, director de investigación del departamento de Tiltman, se acercó a la mesa de Bill Tutte (1917-2002), un estudiante de química de la Universidad de Cambridge, y le dijo *"Mira a ver que puedes hacer con esto ..."*. Tutte, que había sido rechazado en Bletchley Park para la desencriptación de Enigma, fue reclutado por el propio Tiltman para su equipo de criptoanalistas. Tutte ya tenía experiencia en tareas criptoanalíticas con el código Hagelin y la máquina sueca C-36. De inmediato se puso a trabajar para averiguar el funcionamiento de las Lorenz. Paradójicamente, a diferencia de las Enigma, la ruptura del código de las Lorenz fue relativamente más sencilla. Tutte, que estaba muy familiarizado con el método de Kasiski ya que había sido instruido en él durante su fase de reclutamiento, comenzó estudiando patrones de repetición de dicho mensaje. Recordemos que aunque el método de Kasiski estuviera diseñado para romper la cifra Vigènere, podía resultar muy útil en general a la hora de encontrar comportamientos periódicos sistemáticos de la clave en multitud de cifrados. Tutte colocó al principio los caracteres cifrados en código Baudot en vertical en siete filas de 575 caracteres cada una. El porqué utilizó esta cantidad es debido a que al colocar todos los caracteres del mensaje cifrado en un rectángulo, observó ciertas repeticiones primero cada 23 posiciones y después cada 25. Tras multiplicar estos números ($23 \times 25 = 575$), consideró oportuno realizar esta suposición. Al principio no parecía haber demasiadas coincidencias, pero para su sorpresa observó que existían algunas repeticiones en una diagonal, y que parecía que obtendría mejores resultados si configuraba el mensaje con un periodo de 574 caracteres. Así lo hizo y observó con gran satisfacción que se producían un gran número de repeticiones de patrones de longitud 5 o 6. Entonces realizó un nuevo intento con un periodo de 41, ya que éste es un factor primo de 574, y los resultados fueron asombrosamente aún mejores. Poco a poco fue descubriendo la configuración de funcionamiento de las Lorenz, lo cual era sorprendente ya que nunca tuvo delante ninguna de estas máquinas.

La máquina Lorenz contaba con lo que hoy día conocemos como generador de *números aleatorios*, que no es otra cosa que una clase de algoritmo que se utiliza en la programación de los modernos ordenadores para la obtención de números pseudoaleatorios. Desde un punto de vista mecánico cada una de estas ruedas o *pinwheels* poseía un cierto número de posiciones sobre su periferia con un perno o pin que admitía dos posiciones, *on* u *off* (encendido o apagado), que durante el giro de la rueda afectaban o no a otras partes de la máquina generándose secuencias

[45] http://www.newmarketlhs.org.uk/personalities5.htm

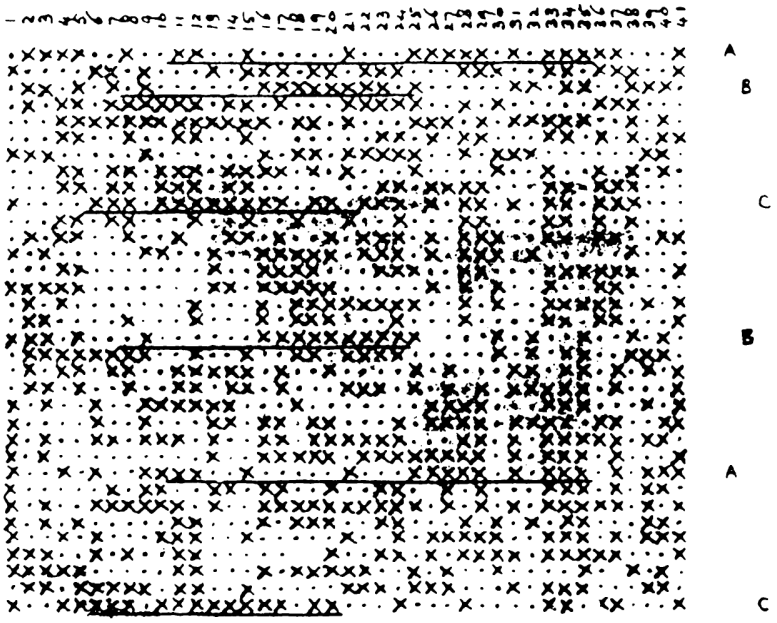

Figura 45. Exámen de periocidad de la rueda χ_1, repeticiones de Kasiski: A, B, C. Secuencias escritas en filas de 41 caracteres de longitud. Manuscrito de Tutte. [1]

de pulsos *on/off* o si se prefiere secuencias de bits $1/0$. El número de pernos o *pins* era variable en cada rueda, de modo que χ_1, χ_2, χ_3, χ_4 y χ_5 tenían 41, 31, 29, 26 y 23 respectivamente, mientras que ψ_1, ψ_2, ψ_3, ψ_4 y ψ_5 presentaban 43, 47, 51, 53 y 59 cada una de ellas, y finalmente las dos ruedas motoras μ_1 y μ_2 contaban con 37 y 61 respectivamente. Las ruedas χ giraban todas una posición para cada carácter. Las ruedas ψ también giraban todas a la vez, pero no con cada carácter. Su movimiento estaba controlado por las dos ruedas motoras μ. En las SZ40 la rueda μ_1 giraba una posición con cada carácter, pero la rueda μ_2 únicamente giraba cuando el *pin* de la periferia estaba en la posición de encendido *on*. Si el *pin* de la rueda μ_2 estaba encendido, entonces todas las ruedas ψ giraban. El orden de las ruedas era (de izquierda a derecha): χ_1, χ_2, χ_3, χ_4, χ_5, μ_2, μ_1, ψ_1, ψ_2, ψ_3, ψ_4, ψ_5. Los modelos SZ42A y SZ42B estaban dotados de un mecanismo aún más complejo. Como puede observarse el número de *pins* de una rueda era un número primo relativo al de otras ruedas, ya que de esta forma se hacía máximo el periodo combinado de todas las ruedas, y de este modo el patrón de repetición. Con un total de 501 *pines*, esto suponía 2^{501} que es aproximadamente 10^{151} posibilidades de cifrado con $1,6 \times 10^{15}$ posiciones iniciales de las ruedas posibles. Sin embargo, si los cinco impulsos se consideraban de manera independiente, los números resultantes eran más manejables. El producto del periodo de rotación de cualquier par de ruedas χ supone entre $41 \times 31 = 1271$ y $26 \times 23 = 598$. Esta clase de ingenio mecánico se considera hoy en día como uno los predecesores de lo que en electrónica y en criptografía se conoce con el nombre de *registros de desplazamiento alimentados linealmente* (en inglés *Linear Feedback Shift Registers*, abreviadamente *LFSK*). Cuatro meses después de haberle sido encomendada la tarea a Tutte, y una vez el código Lorenz había sido descifrado, en Bletchley Park se mandó construir una máquina electro-mecánica, a la que se le bautizó con el nombre de *máquina Tunny*, cuya finalidad era precisamente sistematizar las tareas de descodificación de las Lorenz.

En una primera instancia, Tutte había desarrollado un método para establecer la configuración inicial de las Lorenz "a mano". Sin embargo este método no resultaba operativo, ya que el descifrado de un simple mensaje podía llegar a alargarse varias semanas en el tiempo, por lo que en la mayoría de las ocasiones el mensaje había perdido ya todo el interés, pues hacía referencia a órdenes ya obsoletas, de las cuales era imposible sacar ninguna ventaja desde el punto

de vista estratégico. Por ello, era necesario desarrollar un nuevo método capaz de obtener rápidamente si no el mensaje plano íntegro, sí una gran mayoría de caracteres que ayudaran a la inteligencia británica a adelantarse a los acontecimientos.

En noviembre de 1942, Tutte desarrolló un ingenioso método con el que si bien no se obtenía la traducción exacta de los mensajes, sí que lo hacía en una gran proporción. Este método fue bautizado con el nombre de *Método Estadístico*. Los cálculos necesarios se llevaban a cabo mediante la comparativa de dos secuencias de caracteres en código Baudot, puntos y cruces (similar a 1 y 0 como anteriormente se hizo referencia), y llevando a cabo un recuento del número de veces que cada uno de ellos tenía un punto o una cruz en la misma posición. Tutte puso en conocimiento de Max Newman, jefe de la sección de desarrollo mecánico en Bletchley Park, y éste le sugirió utilizar contadores electrónicos de alta velocidad con el fin de automatizar el proceso.

7. Colossus. El primer ordenador electrónico

Una vez Bill Tutte había formalizado el trabajo de desencriptación del código de las Lorenz, surgía nuevamente la necesidad de sistematizar todas las tareas de desencriptado. Del mismo modo que las *bombe* habían surgido para mejorar la eficacia de las tareas de descifrado de las Enigma, *Colossus* fue construido para lograr una optimización de estas mismas tareas en las máquinas Lorenz. Colossus puede ser considerado en cierto modo, la primera máquina programable, electrónica y digital, y por sus características, aunque con ciertas reservas, se ganó el derecho de ostentar el título de primer ordenador de la historia de la computación.

La idea original para la construcción de Colossus fue desarrollada por el matemático Max Newman (1897-1984) y todo un equipo de técnicos de Bletchley Park, que previamente se habían encargado del desarrollo de la *Heath Robinson* y posteriormente la *Old Robinson*, y la *Super Robinson*, todas ellas máquinas optomecánicas que supusieron un primer intento de sistematizar el método desarrollado por Tutte. Sin embargo las *Robinson* resultaron ser máquinas poco eficientes desde el punto de vista operativo, ya que necesitaban dos cintas, una con el mensaje cifrado y otra con una secuencia de números aleatorios obtenidos a partir de ruedas similares a las de las máquinas Lorenz. Desafortunadamente cuando se intentaba aumentar la velocidad de lectura de datos por encima de los 1.000 caracteres por segundo, esta última cinta se estiraba más de la cuenta, produciendo graves errores. Tommy Flowers (1905-1998), un ingeniero de la *British Post Office Research Station* en Dollis Hill, al noroeste de Londres, fue el encargado de desarrollar el primer prototipo de Colossus. Flowers ya había colaborado previamente en el desarrollo de varios proyectos en Bletchley Park, incluido la invención de algunos componentes de las *bombe* de Turing como los dispositivos rotatorios de alta velocidad. La verdadera genialidad de Flowers en la construcción de Colossus radica fundamentalmente en la utilización de unos nuevos circuitos electrónicos a base de *válvulas* en lugar de los relés tradicionales en la segunda cinta que contenía los números aleatorios, lo cual aumentaba la velocidad de lectura de datos a la vez que la fiabilidad mejoraba ostensiblemente, llegando a conseguir velocidades de lectura de 5.000 caracteres por segundo, lo que suponía unos doce metros de cinta.

El ordenador Colossus llegó a tener unas 1.500 *válvulas*, *tiratrones* y *fotomultiplicadores*. Una *válvula* o tubo de vacío es un componente electrónico que es el antecesor de los actuales diodos y transistores, que en general sirve para incrementar el voltaje dentro de un circuito. El *tiratrón*, otra clase de válvula utilizada en los circuitos de Colossus, era un tubo relleno de gas, por ejemplo neón o xenón. Su comportamiento era el de un rectificador que funcionaba como un interruptor eléctrico. Este dispositivo se utilizaba con el fin de grabar 1 bit. Conectando varios de estos dispositivos entre sí se lograba un circuito, una *memoria*, conocida hoy día como *registro de desplazamiento*, o más comúnmente denominado *tiristor*. Los *fotomultiplicadores* eran un tipo de

[46] http://www.colossus-computer.com/colossus1.html

Figura 46. De izq. a drcha. Max Newman, Tommy Flowers, W. W. Chandler y Donald Mitchie.[46]

válvulas cuya finalidad principal era la detección de luz. Aplicando estos dos últimos componentes, tiratrones y fotomultiplicadores, Colossus era capaz de leer los caracteres de una cinta de papel aplicando una función lógica previamente programada a cada carácter. Si el resultado de aplicar la función lógica era verdadero la lectura de la cinta y el análisis posterior seguían su curso.

En enero de 1944, y tras algo más de un año en construirse, apareció la primera versión de Colossus, denominada Mark I. Rápidamente le siguió la Mark II en junio de ese mismo año. A finales de la 2ª Guerra Mundial, había un total de 10 máquinas Mark II en Bletchley Park. El volumen de dichas máquinas era considerable ya que cada una de ellas ocupaba una gran habitación en los sectores F y H. Al igual que ocurrió con las Bombe, Churchill ordenó su destrucción una vez finalizada la guerra por motivos de seguridad, quemándose todos los planos con el diseño y circuitos. Sin embargo dos de ellas sobrevivieron, trasladándose a Cheltenham, donde fueron utilizadas durante la Guerra Fría hasta que finalmente se ordenó su destrucción en la década de 1960. Debido al secretismo impuesto por las autoridades británicas, tanto Colossus, como sus creadores nunca gozaron del mérito que merecieron en la historia de la computación, ya que la máquina norteamericana ENIAC construida en 1946 y sus creadores fueron los que se llevaron los méritos y el reconocimiento público.

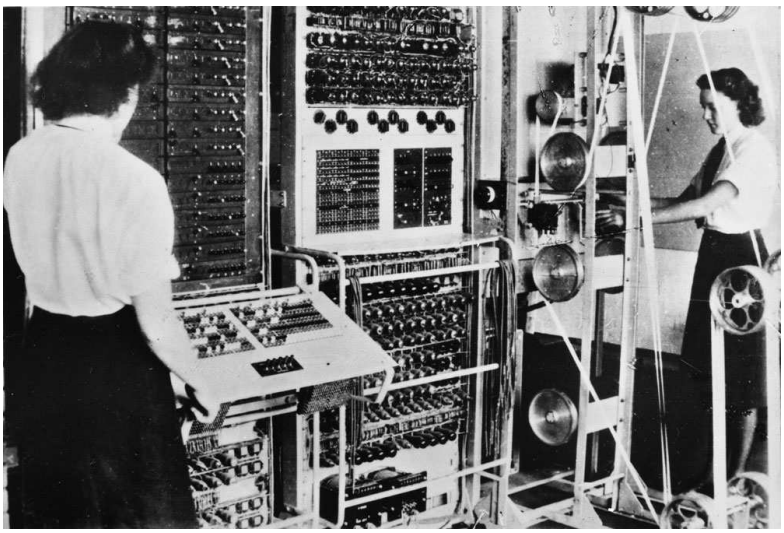

Figura 47. Colossus y dos operadoras del Servicio Naval Real (Royal Naval Service). Dorothy Boisson (izq.) y Elsie Booker (drcha.) (Bletchley Park, 1943).[47]

[47] The National Archives, http://blog.nationalarchives.gov.uk/blog/innovating-at-the-national-archives/

Tony Sale (1931-2011), un antiguo trabajador del servicio británico, fue nombrado conservador del Museo de Bletchley Park al inicio de la década de los 90. Hasta 1993 se dedicó a recopilar cuanta información pudo sobre la máquina Colossus con el fin de comenzar su reconstrucción. En 1994, comenzaban las primeras tareas de reensamblaje eligiéndose además la misma ubicación que una de las máquinas (la número 9) había tenido durante la guerra. Finalmente en 1996, era presentada una primera versión que trabajaba a 2 bits en lugar de los 5 con los que trabajaba la máquina original.

Referencias

[1] BAUER, F. L., *Decrypted Secretsthods and Maxims of Cryotology*, 4th Ed., Springer Verlag, Berlin, 2007.

[2] CEANO, R., *La Máquina Enigma*, http://www.kriptopolis.com/enigma, 2012. (Última consulta 20-11-2012)

[3] COOMBS, A. W. H., *The Making of Colossus*, Annals of the History of Computing, Volume 5, Number 3, july 1983.

[4] COPELAND, J., *Colossus: Its Origins and Originators*, Annals of the History of Computing, pp. 38–44, Computer Society, UK, 2004.

[5] CHRISTENSEN, C., *Polish Mathematicians Finding Patterns in Enigma Messages*, Mathematics Magazine, Nº. 80, pp. 247–273, october 2007.

[6] FERNÁNDEZ, S., *La Criptografía Clásica*, Revista SIGMA, Nº. 24, pp. 119–141, abril 2004.

[7] FLOWERS, T. H., *The Design of Colossus*, Annals of the History of Computing, Volume 5, Number 3, july 1983.

[8] GAJ, K., ORLOWSKI, A. *Facts and myths of Enigma: breaking stereotypes*, EUROCRYPT'03 Proceedings of the 22nd international conference on Theory and applications of cryptographic techniques, Springer-Verlag, Berlin, Heidelberg, pp. 106–122, 2003.

[9] HODGES, A., *The Military Use of Alan Turing*, Mathematics and War, pp. 312–325, Bernhelm Booss Bavnbek and Jens Høyrup Editors, Birkhäuser, 2003.

[10] KERCKHOFFS, A., *La cryptographie militaire*, Journal des sciences militaires, vol. IX, pp. 5—83, jan. 1883, pp. 161—191, fév. 1883.

[11] KOZACZUK, W., *ENIGMA: The Key to the Secrets of the Third Reich 1933-45*, Interpress, june 1984.

[12] LAHOZ-BELTRA, R., *Turing: Del primer ordenador a la inteligencia artificial*, Colección: La matemática y sus personajes, Nº. 24, 1ª Edición. Nívola, Madrid, 2005.

[13] MEDRALA, J., *L'Enigma 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.

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

[15] ORTEGA TRIGUERO, J.J., LÓPEZ GUERRERO, M.A. y GARCÍA DEL CASTILLO CRESPO, E.C., *Introducción a la Criptografía. Historia y Actualidad*, Servicio de Publicaciones de la Universidad de Castilla La Mancha, Colección Monografías, Nº. 50, 2006.

[16] QUIRANTES SIERRA, A., *Enigma: la solución polaca (I) y (II)*, Boletín del Taller de Criptología, Nº. 18, diciembre 2003.

[17] RANDEL, B., *The Colossus*, International Research Conference on the History of Computing, Los Alamos Scientific Laboratory, University of California, June 10-15th, 1976.

[18] REJEWSKI, M., *An Application of the Theory of Permutations in Breaking the Enigma Cipher*, Applicaciones Mathematicae. 16, Nº. 4, Warsaw 1980.

[19] REJEWSKI, M., *How Polish Mathematicians Deciphered the Enigma*, Annals of the History of Computing. Volume 3. Number 3, July 1981.

[20] SÁNCHEZ MUÑOZ, J. M., *Nazis y Matemáticas*, 2ª Jornada Internacional "Matemáticas Everywhere", Castro Urdiales, 20–21 junio, 2012.

[21] SINGH, S., *Los Códigos Secretos: El arte y la ciencia de la criptografía, desde el antiguo Egipto a la era Internet*, Editorial Debate, 2000.

[22] TUTTE, W. T., *Fish and I*, Transcripcción de Conferencia en la Universidad de Waterloo (19 de junio de 1998), Ontario, Canadá, 2012.

[23] UNIÓN INTERNACIONAL DE TELECOMUNICACIONES, *Reglamento Telegráfico, Revisión de Ginebra, 1958*, Anexo al Convenio Internacional de Telecomunicaciones, Buenos Aires, 1952, Protocolo Final, Ginebra, 1959.

[24] VV.AA, *The History of Information Security: A Comprehensive Handbook*, Karl de Leeuw y Jan Bergstra (Editores), Elsevier B.V., 2007.

[25] WESOLKOWSKI, S., *The Invention of Enigma and How the Polish Broke It Before the Start of WWII*. IEEE Conference on the History of Telecommunications, University of Waterloo, Canada, 2001.

Sobre el autor:
Nombre: José Manuel Sánchez Muñoz
Correo electrónico: jmanuel.sanchez@gmx.es
Institución: Ingeniero de Caminos, Canales y Puertos. Grupo de Innovación Educativa "Pensamiento Matemático", Universidad Politécnica de Madrid, España.