Encontrando claves de Enigma con permutaciones

Clara Acosta Villamil

Trabajo de fin de grado en Matemáticas
Universidad de Zaragoza

Directora del trabajo: Paz Jiménez Seral y Manuel Vázquez Lapuente

10 de septiembre de 2021

Abstract

Throughout history, people have coded their messages with the simple intention that these will pass unnoticed and maintain their secrecy. The main disadvantage of this was that anyone could intercept a hidden message and compromise the security of the communication.

To refelct that need, cryptography emerged, whose purpose was more than in hiding the message, to hide its meaning through a coding process. Additionally, there appeared the first analysis techniques whose purpose was to unmask the secret content of encrypted messages. Since its inception, the cryptography found its main usefulness in the war.

At the end of the First World War, the appearance and proliferation of rotor encryption machines occurred. These machines allowed the cryptographers to mechanize the encryption process, making practically inaccessible the tasks of those who were trying to unravel what was hidden behind the encrypted messages with said mechanisms. From all these devices undoubtedly highlights the Enigma machine.

The main objective of this work is to reveal the keys to the successful Polish attack on the enigma protocol starring by Marian Rejewski, whose result was vital for the defeat of the Nazis in World War II. The work is based especially on a detailed description of the grid method, one of the messages decryption procedures that was fundamental to broke Enigma..

After giving a small chronology of how the process of decryption arise adapting to the changes introduced by the Germans, we begin by describing the machine and its operation, where, in addition to detailing each part of the machine and its internal mechanism, we explain the steps they had to follow the Germans to configure the machine for its later use. We also see how each part of the machine translated into new encryption possibilities, increasing the ways to configure it becoming an unbreakable machine in the eyes of the Germans.

In the next chapter we introduce the theory of permutations, giving basic definitions that we will use throughout the work and enuncing some important mathematical results on which Rejewski was based and that were necessary for the attack.

Next, we will illustrate with a detailed example the procedure that followed Rejewski to find key parts in deciphering with the grid method.

Finally, we will expose an invention of the Poles to mechanize the process of decryption, the cyclometer.

Throughout the work, other methods that were used and complemented to those explained in the fight against enigma are also appointed, but we do not develop them, such as the clock method, the ANX method or the Zygalski's sheets.

Índice general

Capítulo 1

Introducción

A principios del siglo XX, la invención de máquinas mecánicas y electromecánicas complejas, como la máquina Enigma, proporcionaron métodos de cifrado sofisticados y eficientes para la protección de la confidencialidad de informaciones militares, políticas y comerciales.

El período donde tomó una vital importancia la máquina Enigma fue en la Segunda Guerra Mundial, convirtiéndose en uno de los inventos más fascinantes de la época.

Tras la Primera Guerra Mundial, los aliados se encargaron de vigilar las comunicaciones alemanas. Pero en 1928 empezaron a tener problemas, ya que interceptaron mensajes cifrados con un nuevo método desconocido hasta el momento. Los informes que se hacían sobre la posibilidad de criptoanalizar los mensajes cifrados con Enigma eran muy pesimistas, lo cual generó un clima de desconfianza. Debido a esto, un cierto número de estudiantes de matemáticas recibieron un llamamiento del ejército polaco para participar en un curso de criptología. Entre esos estudiantes destacan Marian Rejewski, Jerzy Ròzycki y Henryk Zygalski, con los que comenzaba la guerra de los matemáticos contra Enigma.

Mediante permutaciones, Rejewski contruyó el modelo matemático de una máquina Enigma. Además realizó una gran hazaña criptográfica al conseguir el secreto de los cableados de la máquina usada por el ejército alemán.

Debido a la gran cantidad de formas que había de configurar Enigma, conseguir averiguar la correcta era un trabajo manual muy laborioso. Ello motivó a los polacos a construir unas réplicas de la Enigma militar a principios de febrero de 1933, gracias a las cuales pudieron mecanizar la tarea de encontrar las posibles configuraciones de la máquina.

Durante los primeros meses de la primera victoria polaca sobre Enigma, los operarios tenían que obtener la configuración inicial de manera prácticamente manual, teniendo que averiguar las claves del día y el orden de los rotores. La tarea fue tornándose complicada, por lo que Rejewski pidió ayudar a sus compañeros Ròzycki y Zygalski, y conjuntamente diseñaron el ciclómetro, el cual se trataba de una máquina Enigma doble de la que daremos detalles más adelante. Con ayuda de este invento crearon una enciclopedia a base de teclear todas las combinaciones para todas las posiciones de la máquina.

En noviembre de 1937 los alemanes hicieron algunos cambio en la máquina. Pero en septiembre de 1938, Zygalski inventó un método rudimentario aunque bastante efectivo, conocido como las Hojas de Zygalski, a partir del cual Enigma volvía a estar tan indefensa como antes del cambio de procedimiento.

Por otro lado, Ròzycki contribuyó en la lucha desarrollando el método del reloj.

Después de casi siete años de trabajo con Enigma, Rejewski inventó un nuevo aparato para el descifrado, la bomba criptológica. Se trataba de unos aparatos electromecánicos basados en la combinación de 6 réplicas de Enigma.

Todos estos métodos fueron clave para la ruptura de Enigma y los describiremos posteriormente, centrándonos en particular en el método de la rejilla. Este supuso un avance clave en la ruptura de Enigma ya que permitió a los polacos conocer el clavijero, la parte más difícil de averiguar debido a la gran cantidad de posibilidades que tenía.

.

Capítulo 2

La máquina Enigma

En este capítulo introducimos una descripción detallada de cada una de las partes de las que se compone la máquina Enigma así como su funcionamiento.

2.1. Descripción de la máquina Enigma

Figura 2.1: Partes de Enigma

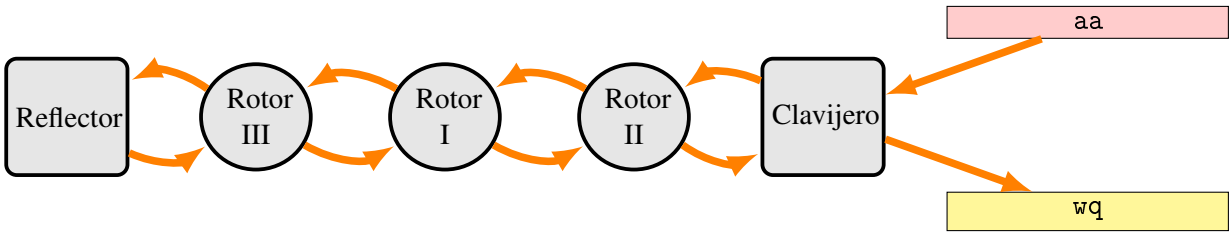
En la Figura 2.1 vemos cómo es la apariencia física de Enigma. Además, podemos observar cada uno de los componentes de la máquina, los cuales decribimos a continuación.

- **Teclado**: compuesto de 26 letras para introducir el texto original.
- **Rotores**: conjunto formado por 3 rotores en secuencia. A partir de 1938 se disponía de cinco, de los cuales elegían tres. Cada rotor es un cilindro con 26 contactos en cada cara. Internamente existen cables que conectan cada contacto de una cara de un rotor con los de la otra cara. A su vez, los contactos de salida de un rotor se conectaban con los contactos de entrada del siguiente. Cada rotor puede girar 26 posiciones antes de cada giro completo. El rotor situado en la derecha giraba un puesto cada vez que una tecla era pulsada, y además, cada rotor mueve un puesto cuando el rotor que está a su derecha ha llegado a una posición establecida previamente, llamada turnover. Los rotores se denominaban como I, II, III, ...
- **Reflector**: emparejaba los 26 contactos dos a dos. Existieron hasta tres reflectores, pero en el período que nos interesa sólo se utiliza el reflector A.
- **Clavijero**: tablero de clavijas, cada una asociada a una letra del alfabeto. Dichas clavijas estaban conectadas mediante 6 cables que podían conmutarse. Más adelante los cables se aumentaron hasta 10.
- **Panel luminoso**: compuesto de 26 luces etiquetadas con letras que muestran el texto cifrado. La letra iluminada era siempre diferente de la tecla pulsada.

Así, al pulsar una de las 26 letras del teclado se cerraba uno de los 26 circuitos de cables y se iluminaba una de las 26 bombillas etiquetadas con letras, dando lugar al resultado del cifrado.

2.2. Funcionamiento de Enigma

El operador debía teclear las letras de su mensaje mientras su ayudante anotaba una a una las letras que le devolvía la máquina iluminadas en el panel de luces. Cada vez que el operador pulsaba una tecla se enviaba un impulso eléctrico que recorría el interior de la máquina tal y como se muestra en el siguiente esquema[1]:



siendo el texto en rojo el introducido por el operario inicialmente (el cual queremos cifrar), y el texto en amarillo el ya cifrado.

Lo primero que debía hacerse para configurar la máquina era elegir la clave que tanto el emisor como el receptor debían usar. Antes de cifrar el mensaje, el operador encargado debía disponer la máquina según la clave del día, la cual figuraba en el cuaderno de claves. Cada una de ellas constaba de los siguientes datos:

Walzenlage	Ringstellung	Stecker	Grundstellung
III I II	XPR	FM:BL:WQ:EA:XO:ZN	DEO

Cuadro 2.1: Configuración real que aparecería en el cuaderno de claves

- Orden de los rotores (*Walzenlage*): elección y colocación de los 3 rotores en el orden adecuado.
- Ajuste: diferenciamos entre dos tipos de ajuste:
  - Interno (*Ringstellung*): daba información de cómo ajustar el anillo que tenía cada rotor a su alrededor con el rotor en sí. Se ajustaba con el rotor fuera de la máquina. Estaba constituido por tres letras, una para cada rotor.
  - Externo (*Grundstellung*): después de estar colocados los rotores en la máquina estos debían girarse hasta quedar reajustados, apareciendo dicho ajuste a través de las ventanillas. Esta clave constaba de otras tres letras.
- Conexiones del clavijero (*Stecker*).

Los pasos que debía seguir el emisor para el proceso de cifrado eran los siguientes:

Primer paso: Debía configurar Enigma con la clave del día según el Diario de Claves.

Segundo paso: Con el fin de que todos los mensajes de un mismo día no fueran cifrados con la misma clave, el emisor elegía al azar tres letras que constituirían la clave del mensaje. El emisor necesitaba enviar al receptor esa clave del mensaje (*Spruchschlüssel*), para ello previamente cifraba las tres letras

[1] Los rotores se ordenaban según la clave del día, en este ejemplo hemos elegido el orden III, I, II

dos veces con el ajuste externo que figuraba en el diario de claves, obteniendo así 6 letras que serían el principio del mensaje enviado.

Tercer paso: Debía girar los rotores desde su posición inicial *(Grundstellung)* a la posición de esas tres letras *(Spruchschlüssel)*.

Cuarto paso: Por último, el emisor procedía a codificar el mensaje a enviar, escribiéndolo después de las 6 letras de la clave cifrada.

El receptor, teniendo la máquina configurada según el Diario de Claves, tecleaba las 6 primeras letras y veía en el panel de luces las escritas inicialmente por el emisor, es decir, la clave del mensaje repetida dos veces. Entonces procedía a girar los rotores a esa disposición y tecleaba el resto del mensaje obteniendo el original. Si al teclear las 6 letras la clave no aparecía repetida, esto significaba que había habido un error en la trasmisión, por lo que se solicitaba volver a enviarlo.

En cada momento la letra que se iluminaba dependía no solo de la tecla que se pulsaba, sino también de la configuración de la máquina en ese momento. Concretamente de los recorridos de los 26 circuitos que terminaban en las bombillas. Esos circuitos dependían de la elección de los 3 rotores y de las formas de colocarlos y ordenarlos. Una vez colocado el rotor, el recorrido de los cables dependía de la distancia entre las letras del ajuste interno y externo, lo que se conoce como *ajuste conjunto*. Numerando las letras de los ajustes de los anillos como `A`=1, `B`=2, ..., `Z`=26, el ajuste conjunto se representa como una terna de números del 1 al 26 y se obtiene restando el interno menos el externo, escrito en módulo 26. Con los ajustes del cuadro 2.1, el ajuste conjunto es `(D-X, E-P, O-R)`.
El recorrido también dependía de las parejas formadas con los 6 cables del clavijero entre las 26 letras. Teniendo así

$$26^3 \cdot 6 \cdot \frac{26!}{14!2^6} \approx 7{,}62 \times 10^{18}$$

posibilidades de configurar la máquina:

La letra se iluminaba dependiendo de los ajustes de la máquina, por lo que, para cualquier orden dado de los rotores, se tenían $26 \cdot 26 \cdot 26 = 17576$ posibilidades, ya que cada rotor podía colocarse de 26 formas distintas, una por cada letra del abecedario.
La forma de colocar los tres rotores en las tres hendiduras daba lugar a $3 \cdot 2 \cdot 1 = 6$ posiciones diferentes en las que se pueden colocar los rotores.
El clavijero intercambia 6 pares de letras, pero el intercambio `(a b)` sería igual a `(b a)`, por lo que el número de combinaciones debido a las clavijas sería:

$$\frac{26 \cdot 25}{2}\frac{24 \cdot 23}{2}\frac{22 \cdot 21}{2}\frac{20 \cdot 19}{2}\frac{18 \cdot 17}{2}\frac{16 \cdot 15}{2}$$

Cuando se pulsa una letra del teclado, el rotor derecho avanza 1/26 parte de una vuelta, y si su pestaña está en la posición adecuada (turnover) a su vez provoca que avance el segundo rotor, y lo mismo con el tercero. Además, estos dos últimos rotores también giraban cuando llegaban a la posición de su propio turnover. Las posiciones de turnover dependían de qué letra estaba en la ventanilla, las cuales se llamaban *letras del turnover* de cada rotor. Para el rotor I, su letra de turnover era la `Q`, para el rotor II la `E` y para el rotor III la `V`.

Debido a esta variación de la configuración de la máquina cada vez que se pulsa una tecla, se comprende que una misma letra pulsada dos veces se cifraba en dos letras distintas, por ejemplo, con la configuaración del cuadro anterior, si en el mensaje inicial aparece `aa`, el mensaje cifrado sería, `wq`.

Normalmente se necesitaban dos personas para operar la máquina, una que pulsaba el teclado con el mensaje original y otra que apuntaba las letras de las lámparas que se iluminaban y que describían el mensaje cifrado.

Capítulo 3

Las matemáticas necesarias para el ataque

Rejewski se basó en la teoría de grupos de permutaciones para descifrar Enigma, tal y como explica en [1]. De hecho formuló un teorema conocido como el Teorema de Rejewski, el cual veremos más adelante. Veamos algunos conceptos necesarios para entender el proceso de romper Enigma:

3.0.1. Permutaciones

Sea $\mathscr{C}$ un conjunto no vacío, una *permutación* de $\mathscr{C}$ es una aplicación biyectiva de $\mathscr{C}$ en sí mismo. Los elementos de $\mathscr{C}$ se llaman *letras*.
Nos interesa el conjunto $\mathscr{C} = \{a, b, \ldots, z\}$, es decir, el formado por las 26 letras del alfabeto.
Para indicar que una permutación α lleva la letra i a la letra j, lo denotamos como $i\alpha = j$. Si $i \neq j$, decimos que α mueve i a j; en caso contrario, se dice que α fija i.
Una forma de representar una permutación α es mediante una matriz de correspondencias, en la que se escribe el alfabeto ordenado y debajo las imágenes de cada letra por α, de la forma:

$$\begin{pmatrix} a & b & \ldots & z \\ a\alpha & b\alpha & \ldots & z\alpha \end{pmatrix}$$

Otra forma de representarla es mediante producto de ciclos que mueven letras distintas, es decir, que son *disjuntos*. Una permutación α es un *ciclo* de longitud r, o un *r-ciclo*, si existen r letras diferentes y ordenadas tal que α mueve cada una a la siguiente, la última a la primera, y fija cualquier otra letra. Esto se denota como $\alpha = (c_1\, c_2 \ldots c_r)$ teniendo $c_i\alpha = c_{i+1}, c_r\alpha = c_1$ y fija el resto de las letras que estén en el conjunto pero no aparezcan en α. Claramente un ciclo está determinado por esas letras y su ordenación, salvo por su ordenación cíclica, es decir, $(c_1\, c_2 \ldots c_r) = (c_r\, c_1\, c_2 \ldots c_{r-1})$.

La demostración de la siguiente proposición puede verse en la sección 3 de [7]:

Proposición 3.1. *Toda permutación se puede expresar como producto de ciclos disjuntos incluyendo todas las letras. Estos ciclos disjuntos se dice que forman parte de la permutación. Esta factorización es única salvo el orden en el que los ciclos están escritos.*

La composición de las permutaciones α y β es claramente permutación, llamada *producto* y se denota $\alpha\beta$. De acuerdo a la notación a izquierdas, actuaría primera α y luego β.

Ejemplo 3.1. En este ejemplo vemos las dos formas de expresar una permutación. A lo largo del trabajo

usaremos las dos notaciones, indicándolo en cada caso.

$$\begin{pmatrix} abcdefghijklmnopqrstuvwxyz \\ ekmflgdqvzntowyhxuspaibrcj \end{pmatrix} = (aeltphqxru)(bknw)(cmoy)(dfg)(iv)(jz)(s)$$

En el caso $r=1$, un 1-ciclo es la aplicación identidad ι, la cual deja fija todas las letras.
Ciclos de longitud 2 se llaman *trasposiciones*.

En general, $\alpha\beta \neq \beta\alpha$. Veamos un ejemplo:
Sean

$$\alpha = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}, \beta = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$$

Entonces,

$$\alpha\beta = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}$$

Mientras que

$$\beta\alpha = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}$$

Dos permutaciones se dicen *disjuntas* si no tienen letras en común. Si las permutaciones α y β son disjuntas, entonces $\alpha\beta = \beta\alpha$. Por ejemplo:

$$(abc)(de) = (de)(abc)$$

La longitud de cada uno de los ciclos disjuntos obtenidos, escrita en forma decreciente, se llama *tipo*. En nuestro ejemplo 3.1, el tipo de la permutación es (10, 4, 3, 2, 2, 1).

Llamaremos *orden* de una permutación α al menor número natural r tal que $\alpha^r = \iota$.

Proposición 3.2. *El orden de un ciclo de longitud r es igual a r. El orden de una permutación α es igual al mínimo común múltiplo de las longitudes de los ciclos disjuntos en los que se descompone α.*

Demostración: Inmediata.

Así, el orden de la permutación de nuestro ejemplo 3.1 es mcm(10, 4, 3, 2, 2, 1) = 60.

Como una permutación α es una aplicación biyectiva, entonces existe la permutación *inversa* α^{-1} tal que $\alpha\alpha^{-1} = \iota = \alpha^{-1}\alpha$. Por ejemplo

$$(c_1 c_2 \dots c_r)^{-1} = (c_r c_{r-1} \dots c_2 c_1)$$

Una *involución* es una permutación α de orden 2, es decir, tal que $\alpha \neq \iota$ y $\alpha^2 = \iota$. En este caso, $\alpha = \alpha^{-1}$. Además, se comprueba fácilmente que una permutación es de orden 2 (involución) $\Leftrightarrow$ es producto de trasposiciones disjuntas.

3.0.2. Conjugados

Dos permutaciones α y β se dicen *conjugadas* si existe una permutación γ tal que

$$\alpha = \gamma^{-1}\beta\gamma = \beta^{\gamma}$$

Veamos un ejemplo de conjugación que usaremos en el siguiente capítulo:

.

Ejemplo 3.2. Si tenemos las permutaciones $\pi^{-1} = \texttt{(zyxwvutsrqponmlkjihgfedcba)}$ y $\nu = \texttt{(aeltphqxru)(bknw)(cmoy)(dfg)(iv)(jz)}$. Queremos calcular $\nu^{\pi^{-1}} = (\pi^{-1})^{-1}\nu\pi^{-1} = \pi\nu\pi^{-1}$.

En esta tabla vemos cómo se ve afectada cada letra por la conjugación.

$\xrightarrow{\pi}$	$\xrightarrow{\nu}$	$\xrightarrow{\pi^{-1}}$	
a	b	k	j
b	c	m	l
c	d	f	e
d	e	l	k
e	f	g	f
f	g	d	c
g	h	q	p
h	i	v	u
i	j	z	y
j	k	n	m
k	l	t	s
l	m	o	n
m	n	w	v
n	o	y	x
o	p	h	g
p	q	x	w
q	r	u	t
r	s	s	r
s	t	p	o
t	u	a	z
u	v	i	h
v	w	b	a
w	x	r	q
x	y	c	b
y	z	j	i
z	a	e	d

Cuadro 3.1: Conjugaciones correspondientes a $\pi\nu\pi^{-1}$

Por tanto, $\nu^{\pi^{-1}} = (\pi^{-1})^{-1}\nu\pi^{-1} = \pi\nu\pi^{-1} = \texttt{(ajmv)(blnx)(cef)(dksogpwqtz)(hu)(iy)}$

Proposición 3.3. *Propiedades:*

1. $(\alpha\beta)^\gamma = \alpha^\gamma\beta^\gamma$.
2. $(\beta^\gamma)^{-1} = (\beta^{-1})^\gamma$.
3. $(\beta^\gamma)^\delta = \beta^{\gamma\delta}$.
4. *Si* $\alpha = \beta^\gamma$, *entonces* $\alpha^{\gamma^{-1}} = \beta$.
5. $(c_1\, c_2 \ldots c_r)^\gamma = (c_1\gamma\, c_2\gamma \ldots c_r\gamma)$.
6. *Dos permutaciones conjugadas tienen el mismo tipo.*
7. *Dos permutaciones del mismo tipo son conjugadas.*

.

8. *Si α y β son conjugadas, el número de permutaciones que conjugan una en otra es*

$$\#\{\gamma|\alpha=\beta^{\gamma}\}=r_1r_2\cdots r_st_1!\cdots t_m!,$$

donde $(r_1,r_2,\ldots,r_s)$ es el tipo común de las dos permutaciones y $t_1,\ldots,t_m$ representan las coincidencias de números en ese tipo común.

Demostración: Las primeras propiedades son inmediatas. Para 6 y 7 ver sin mucha dificultad [7] p.47.

El apartado 5 de esta proposición se conoce como el «teorema que permitió ganar la Segunda Guerra Mundial».

Por último, enunciemos el Teorema de Rejewski (ver [8], p. 262), el cual no usamos a lo largo del trabajo pero fue muy importante para conseguir los datos de los que partiremos:

Teorema 3.3. *a. El producto de dos r-ciclos disjuntos es producto de dos involuciones, más concretamente*

$$(c_1\,c_3\,c_5\ldots c_{2r-1})(c_{2r}\,c_{2r-2}\ldots c_4\,c_2)=[(c_1\,c_2)(c_3\,c_4)\ldots(c_{2r-1}\,c_{2r})][(c_2\,c_3)(c_4\,c_5)\ldots(c_{2r}\,c_1)].$$

b. Si las permutaciones α y β son involuciones sin puntos fijos, entonces cada número que forma parte del tipo de $\alpha\beta$ aparece un número par de veces.

c. Si α y β son involuciones sin puntos fijos y la trasposición $(c_1\,c_2)$ forma parte de α, entonces las cifras c_1 y c_2 pertenecen a distintos ciclos de la misma longitud de entre los que forman parte de $\alpha\beta$ (y de $\beta\alpha$).

d. Si α y β son involuciones sin puntos fijos y la trasposición $(c\,c')$ forma parte de α y

$$(\ldots c_1\,c\,c_2\ldots)(\ldots c_1'\,c'\,c_2'\ldots)\subset\alpha\beta,$$

entonces la trasposición $(c_1\,c_2')$ también forma parte de α y la $(c\,c_2')$ de β.

e. Si γ es una permutación tal que cada número de su tipo aparece un número par de veces, entonces $\gamma=\alpha\beta$, con α y β involuciones sin puntos fijos.

3.0.3. Enigma con permutaciones

Con una configuración concreta de la máquina, los 26 circuitos mencionados en el Capítulo 3 relacionan las 26 teclas con las 26 bombillas. Tenemos pues una permutación de las 26 letras del abecedario: `a, b, c, ..., z`. Al pulsar una tecla se ilumina la letra correspondiente por esa permutación. Por el efecto del giro del rotor derecho, la máquina queda constituida de una forma distinta, por ello la permutación cambia cada vez que una letra era pulsada.

Los rotores en posición de ajuste conjunto 0 y el reflector los podemos describir mediante las siguientes permutaciones como producto de ciclos disjuntos[1]:

- Rotor I = `(aeltphqxru)(bknw)(cmoy)(dfg)(iv)(jz)`
- Rotor II = `(fixvyomw)(cdklhup)(esz)(bj)(gr)(nt)`
- Rotor III = `(abdhpejt)(cflvmzoyqirwukxsg)`
- Reflector A = `(ae)(bj)(cm)(dz)(fl)(gy)(hx)(iv)(kw)(nr)(oq)(pu)(st)`

[1] Configuración real de la máquina

Llamamos:

- λ: permutación causada por el rotor izquierdo.
- μ: permutación causada por el rotor central.
- ν: permutación causada por el rotor derecho.
- ρ: permutación causada por el reflector. Producto de 13 trasposiciones disjuntas. En todo nuestro trabajo se supone que ρ se corresponde al reflector A.
- σ: permutación causada por el clavijero. Por ejemplo, el clavijero descrito en la página 4, escrito en lenguaje de permutaciones sería `(mf)(bl)(wq)(ea)(xo)(zn)`. Notar que $\sigma = \sigma^{-1}$.

Así, conocido el recorrido que se realizaba al pulsar una tecla, la permutación que reflejaba este efecto se puede expresar como:

$$\alpha = \sigma\,\nu\,\mu\,\lambda\,\rho\,\lambda^{-1}\,\mu^{-1}\,\nu^{-1}\,\sigma^{-1} = \sigma\,\nu\,\mu\,\lambda\,\rho\,(\sigma\,\nu\,\mu\,\lambda)^{-1}$$

Es decir, que la permutación de Enigma es una conjugada del reflector, y por la proposición 3.3, α consiste en 13 trasposiciones disjuntas.

La representación anterior es una simplificación, ya que la permutación de cada rotor dependía, como se ha dicho en la página 5, del ajuste conjunto.

Como los cables de los rotores están colocados en una especie de circunferencia que puede quedar en distintas posiciones dentro de la máquina, introducimos otra permutación que tiene esto en cuenta:

$$\pi = (\texttt{abcdefghijklmnopqrstuvwxyz}).$$

Esta permutación es un 26-ciclo.

Si la permutación producida por un rotor con ajuste conjunto 0 es ν, con ajuste conjunto 1 será $\pi\nu\pi^{-1}$. Asimismo, cuando el ajuste conjunto sea 2 la permutación será $\pi^2\nu\pi^{-2}$. Y así sucesivamente. Denotamos:

- α_1: permutación que indica cómo cambian las letras cuando se pulsa una tecla por primera vez.
- α_2: permutación que indica cómo cambian las letras cuando se pulsa una tecla por segunda vez, ya que debido al nuevo movimiento del rotor derecho la permutación anterior se modifica.
  ⋮
- α_i: permutación que indica cómo cambian las letras cuando se pulsa una tecla por i-ésima vez.
  ⋮

Así, si por ejemplo, el ajuste conjunto es `(a,b,c)`, la permutación α_i es:

$$\alpha_i = \sigma\pi^{c+i}\nu\pi^{-c-i}\pi^{b}\mu\pi^{-b}\pi^{a}\lambda\pi^{-a}\rho\pi^{a}\lambda^{-1}\pi^{-a}\pi^{b}\mu^{-1}\pi^{-b}\pi^{c+i}\nu^{-1}\pi^{-c-i}\sigma \tag{3.1}$$

Esta expresión se conoce como *Permutación Enigma* correspondiente a una determinada clave. Notar que la máquina Enigma movía una posición antes de codificar, y por lo tanto, el ajuste conjunto del rotor derecho al pulsar una tecla por primera vez pasa de `c` a `c + 1`.

Para aligerar la notación, llamamos $\chi = \mu\pi^{-b}\pi^{a}\lambda\pi^{-a}\rho\pi^{a}\lambda^{-1}\pi^{b}\pi^{-a}\mu^{-1}$. Así, tenemos:

$$\alpha_i = \sigma\pi^{c+i}\nu\pi^{-c-i}\chi\pi^{c+i}\nu^{-1}\pi^{-c-i}\sigma, \qquad i = 1,2,\cdots \tag{3.2}$$

.

La permutación χ es la misma mientras no se muevan los rotores centrales e izquierdo.

Veamos un ejemplo de lo que ocurre al presionar una tecla en el tablero hasta su posterior cifrado.

Ejemplo 3.4. Suponemos que la máquina está configurada como en el cuadro 2.1, siendo el ajuste interno XPR, el externo DEO, y por tanto el conjunto, si numeramos las letras del abecedario del 1 al 26, es (-20, -11, -3), que escrito en módulo 26 es (6, 15, 23). Tenemos además ($\lambda\ \mu\ \nu$) = (RotorIII RotorI RotorII).

Sabemos que la permutación Enigma es:

$$\alpha_i = \sigma\pi^{c+i}\nu\pi^{-c-i}\pi^{b}\mu\pi^{-b}\pi^{a}\lambda\pi^{-a}\rho\pi^{a}\lambda^{-1}\pi^{-a}\pi^{b}\mu^{-1}\pi^{-b}\pi^{c+i}\nu^{-1}\pi^{-c-i}\sigma \tag{3.3}$$

Como sólo vamos a cifrar una letra, nuestro i es 1, y por tanto,

$$\alpha_1 = \sigma\pi^{24}\nu\pi^{-9}\mu\pi^{-9}\lambda\pi^{-6}\rho\pi^{6}\lambda^{-1}\pi^{9}\mu^{-1}\pi^{9}\nu^{-1}\pi^{2}\sigma$$

En el siguiente cuadro mostramos las permutaciones correspondientes al clavijero, los rotores y el reflector escritas en forma de matriz de correspondencia, viendo las imágenes de cada una de las letras del abecedario debajo de las mismas:

Clavijero	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 e l c d a m g h i j k b f z x p w r s t u v q o y n
Rotor II	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 a j d k s i r u x b l h w t m c q g z n p y f v o e
Rotor I	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 e k m f l g d q v z n t o w y h x u s p a i b r c j
Rotor III	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 b d f h j l c p r t x v z n y e i w g a k m u s q o
Reflector A	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 e j m z a l y x v b w f c r q u o n t s p i k h g d

Así, vemos que si pulsamos, por ejemplo a, el camino que sigue la letra es[2]:

$$a \xrightarrow{\sigma} e \xrightarrow{\pi^{24}} c \xrightarrow{\nu} d \xrightarrow{\pi^{-9}} u \xrightarrow{\mu} a \xrightarrow{\pi^{-9}} r \xrightarrow{\lambda} w \xrightarrow{\pi^{-6}} q \xrightarrow{\rho} o \xrightarrow{\pi^{6}} u \xrightarrow{\lambda^{-1}} w \xrightarrow{\pi^{9}} f \xrightarrow{\mu^{-1}} d \xrightarrow{\pi^{9}} m \xrightarrow{\nu^{-1}} o \xrightarrow{\pi^{2}} q \xrightarrow{\sigma} w$$

De esta forma a se cifraba como w, tal y como hemos visto en el esquema del capítulo 2.2.

[2]La conjugación se puede seguir actuando de la misma forma que la vista en el ejemplo 3.2

Capítulo 4

Rompiendo Enigma

En enero de 1933, Rejewski había conseguido obtener los cableados de los rotores y los demás detalles de las máquinas usadas por los alemanes, por lo que no fue difícil que el taller que trabajaba para los servicios secretos polacos pudiera replicar la máquina Enigma. Con ella y usando los métodos que describiremos a continuación día tras día, obtuvieron las claves diarias.

Sabemos que las seis primeras letras de un mensaje cifrado corresponden a la clave del mensaje cifrada dos veces. Las seis permutaciones que cifraban esas 6 letras eran comunes a todos los mensajes de un mismo día. Rejewski fue capaz de encontrar esas seis primeras permutaciones cuando contaba con suficientes mensajes de un mismo día reconstruyendo los productos $\alpha_1\alpha_4, \alpha_2\alpha_5$ y $\alpha_3\alpha_6$ (ver [1]).

El teorema de Rejewski citado en el capítulo anterior nos ayuda a conocer las permutaciones α_i, puesto que las parejas de letras que forman las trasposiciones de α_1 y α_4 se obtienen emparejando dos letras de dos ciclos de la misma longitud de entre los que aparecen en el producto $\alpha_1\alpha_4$. Una vez obtenida una de esas parejas, sabemos cómo obtener el resto (recordar que siempre se empareja la de delante con la de detrás). Es pues necesario conocer previamente alguna trasposición de estas α_i. Rejewski solucionó ese obstáculo intuyendo que algunas claves serían de la forma `aaa, bbb, abc,` etc. Se puede ver un ejemplo de este procedimiento en [2].

4.0.1. Método de la rejilla

En el período inicial de uso de Enigma el orden de los rotores en la máquina se cambiaba cada trimestre y la prioridad era determinar de manera eficiente el ajuste de los rotores y el clavijero. Este último era el más complicado debido a la gran cantidad de posibilidades que había de configurarlo. Con el fin de encontrarlo se desarrolló el método de la rejilla.

Partimos del conocimiento del cableado de rotores y las seis primeras permutaciones α_i.[1]

Descripción de la rejilla

Para este método se necesitaban dos hojas.

[1] Dichas permutaciones α_i eran encontradas previamente gracias a los indicadores como se ha dicho unos párrafos más arriba.

- La hoja superior (rejilla) tenía 6 ranuras, encima de las cuales estaban escritas las permutaciones $\alpha_1, \ldots, \alpha_6$ en forma de matriz de correspondencia.
- La hoja inferior era la correspondiente a los rotores. Había tres hojas, una para cada rotor. Para construir la hoja correspondiente a ν se necesitan las permutaciones del rotor con los distintos ajustes conjuntos posibles, es decir, $\pi^i \nu \pi^{-i}$, i = 0,...,25. Estas permutaciones aparecen escritas también como matriz de correspondencias pero mostrando únicamente las imágenes de las letras del abecedario (la segunda línea de la matriz).

Veamos un ejemplo en el que mostramos ambas hojas:

Ejemplo 4.1. Partimos de las siguientes α_i escritas como producto de ciclos disjuntos:

$$\begin{aligned}
\alpha_1 &= \texttt{(af)(bv)(cw)(dy)(ez)(gp)(hs)(in)(jo)(kx)(lu)(mr)(qt)}\\
\alpha_2 &= \texttt{(aj)(bw)(ce)(dz)(fh)(gx)(in)(km)(lt)(oq)(pu)(ry)(sv)}\\
\alpha_3 &= \texttt{(ao)(bm)(ch)(dx)(ep)(fv)(gy)(iz)(jq)(ku)(ln)(rs)(tw)}\\
\alpha_4 &= \texttt{(ah)(be)(cq)(do)(fs)(gl)(iz)(jp)(kn)(mx)(ry)(tv)(uw)}\\
\alpha_5 &= \texttt{(an)(bt)(cu)(dv)(ek)(fw)(gp)(hx)(ir)(jy)(ls)(mz)(oq)}\\
\alpha_6 &= \texttt{(am)(bl)(cn)(dz)(ew)(fo)(gp)(hy)(ix)(jt)(ks)(qr)(uv)}
\end{aligned}$$

a partir de las cuales se contruye la hoja superior o rejilla:

	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
α_1	f	v	w	y	z	a	p	s	n	o	x	u	r	i	j	g	t	m	h	q	l	b	c	k	d	e
	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
α_2	j	w	e	z	c	h	x	f	n	a	m	t	k	i	q	u	o	y	v	l	p	s	b	g	r	d
	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
α_3	o	m	h	x	p	v	y	c	z	q	u	n	b	l	a	e	j	s	r	w	k	f	t	d	g	i
	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
α_4	h	e	q	o	b	s	l	a	z	p	n	g	x	k	d	j	c	y	f	v	w	t	u	m	r	i
	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
α_5	n	t	u	v	k	w	p	x	r	y	e	s	z	a	q	g	o	i	l	b	c	d	f	h	j	m
	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
α_6	m	l	n	z	w	o	p	y	x	t	s	b	a	c	f	g	r	q	k	j	v	u	e	i	h	d

Por otra parte, las conexiones correspondientes al rotor I con los distintos ajustes son:

$$\begin{aligned}
\pi^0 \nu \pi^{-0} &= \texttt{(aeltphqxru)(bknw)(cmoy)(dfg)(iv)(jz)}\\
\pi \nu \pi^{-1} &= \texttt{(ajmv)(blnx)(cef)(dksogpwqtz)(hu)(iy)}\\
\pi^2 \nu \pi^{-2} &= \texttt{(akmw)(bde)(cjrnfovpsy)(gt)(hx)(iluz)}\\
&\vdots\\
\pi^{25} \nu \pi^{-25} &= \texttt{(ak)(bfmuqirysv)(clox)(dnpz)(egh)(jw)}
\end{aligned}$$

Las filas de abajo de la matriz de correspondencia tal y como aparecerían en la hoja inferior son las

.

siguientes. Para denotar cada permutación ponemos un subíndice al rotor ν según cada ajuste conjunto.

$$\begin{aligned} \nu_0 = \pi^0 \nu \pi^{-0} &: \texttt{ekmflgdqvzntowyhxuspaibrcj} \\ \nu_1 = \pi \nu \pi^{-1} &: \texttt{jlekfcpuymsnvxgwtrozhaqbid} \\ &\vdots \\ \nu_{25} = \pi^{25} \nu \pi^{-25} &: \texttt{kflngmherwaoupxziyvtqbjcsd} \end{aligned}$$

El método consistía en deslizar la rejilla sobre la hoja inferior de tal manera que a través de las ranuras se verían las distintas permutaciones del rotor ν, teniendo una correspondencia entre las α_i y dichas conexiones para cada i. Lo que se pretendía con ello era buscar la posición adecuada en la que se cumplen determinadas condiciones para saber cuál era el ajuste conjunto que se había usado. Además, sabemos que los ajustes de $\alpha_1, \ldots, \alpha_6$ van seguidos, es decir, si el ajuste de α_1 es c+1, el de α_2 será c+2, y así sucesivamente.

Para explicar lo que ocurre partimos de la permutación Enigma 3.1. Suponemos además que no ha habido turnover en las seis primeras permutaciones, es decir, que no ha habido movimiento de los rotores central e izquierdo, lo cual es probable porque sólo se movían una vez cada 26 letras. Tenemos

$$\alpha_i = \sigma\, \pi^{c+i}\, \nu\, \pi^{-c-i}\, \chi\, \pi^{c+i}\, \nu^{-1}\, \pi^{-c-i}\, \sigma = \sigma\, \nu_{c+i}\, \chi\, \nu_{c+i}^{-1}\, \sigma, i = 1, \cdots, 6$$

siendo $\nu_{c+i} = \pi^{c+i}\, \nu\, \pi^{-c-i}$, con c el valor del ajuste conjunto del rotor derecho e i la i-ésima vez que se pulsaba una tecla para su cifrado.

Desconocemos cuál es el rotor derecho, por tanto desconocemos ν. Debido a lo cual esta operación debía realizarse tres veces, una para cada rotor. Una vez que se conocía el rotor derecho, seguimos desconociendo su ajuste conjunto c.

No se conocen σ ni χ (que es producto de trasposiciones ya que es conjugada del reflector). Denotamos $\overline{\alpha_i} = \nu_{c+i}\, \chi\, \nu_{c+i}^{-1}$, que será también producto de trasposiciones disjuntas y que también desconocemos. Además sabemos que $\alpha_i = \sigma\, \nu_{c+i}\, \chi\, \nu_{c+i}^{-1}\, \sigma$. Con esto vemos que α_i y $\overline{\alpha_i}$ son conjugadas por σ.

El clavijero está formado por 6 trasposiciones, por lo que σ dejará las otras 14 letras fijas. Así, las trasposiciones que forman α_i y quedan fijas por el clavijero coincidirán con una trasposición de $\overline{\alpha_i}$. O lo que es lo mismo, algunas trasposiciones de $\nu_{c+i}^{-1}\, \alpha_i\, \nu_{c+i}$ coincidirán con algunas de χ, que es igual a $\nu_{c+i}^{-1}\, \overline{\alpha_i}\, \nu_{c+i}$.

Llamamos

$$\chi_i = \nu_{c+i}^{-1}\, \alpha_i\, \nu_{c+i} \tag{4.1}$$

Sabemos que χ está formada por 13 parejas. Cuando el ajuste conjunto c es el correcto, es muy probable que algunas de las trasposiciones de χ aparezcan repetidas en varias χ_i. Por esa razón buscaremos el c correcto mirando en qué posición hay más trasposiciones repetidas en varias χ_i. Recordemos que desconocemos χ pero podemos conocer las χ_i gracias a que disponemos de todos los datos. Además, la rejilla nos ayuda a conocerlas con más comodidad, como veremos en el siguiente ejemplo.

Ejemplo 4.2. Veamos lo que mostraría la rejilla para las permutaciones α_i descritas antes si usamos el ajuste conjunto $c = 11$, que en nuestro caso es el correcto. Conociéndolo, podemos escribir

$$\alpha_i = \sigma\, \nu_{11+i}\, \chi\, \nu_{11+i}^{-1}\, \sigma \tag{4.2}$$

.

Por tanto, la posición correcta es colocando α_1 en la posición ν_{12}, y veremos que es en la que tenemos más trasposiciones repetidas.

Utilizamos la notación de matriz de correspondencia, escribiendo las letras del abecedario en la primera línea y su imagen por α_i en la segunda línea. La tercera fila es la que es visible a través de la rejilla, y el número que aparece al lado se refiere a la línea de la rejilla correspondiente, es decir, cada permutación del rotor ν:

```
α1 : abcdefghijklmnopqrstuvwxyz
     fvwyzapsnoxurijgtmhqlbckde
12   ckmvligdowpfqxsyatzurejnbh

α2 : abcdefghijklmnopqrstuvwxyz
     jwezchxfnamtkiquoyvlpsbgrd
13   jlukhfcnvoepwrxzsytqdimagb

α3 : abcdefghijklmnopqrstuvwxyz
     omhxpvyczqunblaejsrwkftdgi
14   ktjgebmundovqwyrxspchlzfai

α4 : abcdefghijklmnopqrstuvwxyz
     heqobslazpngxkdjcyfvwtumri
15   sifdaltmcnupvxqwrobgkyezhj

α5 : abcdefghijklmnopqrstuvwxyz
     ntuvkwpxryeszaqgoilbcdfhjm
16   heczkslbmtouwpvqnafjxdygir

α6 : abcdefghijklmnopqrstuvwxyz
     mlnzwopyxtsbacfgrqkjvueihd
17   dbyjrkalsntvoupmzeiwcxfhqg
```

Uso de la rejilla para calcular χ_i

Veamos cómo obtener las trasposiciones disjuntas de χ_i con la rejilla. Lo que obtendremos serán las χ_i de 4.1. Lo que hacemos es conjugar los α_i y el rotor I, es decir, aplicamos $\nu_{11+i}^{-1}\alpha_i\nu_{11+i}$. Veámoslo en el caso anterior calculando χ_1:

La permutación ν_{12}^{-1} lleva `d` a `h`, α_1 podemos ver que intercambia `(h s)`, y ν_{12} lleva `s` a `z`. Por tanto la permutación χ_1 tendrá la trasposición `(d z)`.

```
α1 : abcdefghijklmnopqrstuvwxyz
     fvwyzapsnoxurijgtmhqlbckde
12   ckmvligdowpfqxsyatzurejnbh
```

Con la rejilla esto es muy visual, las dos parejas iguales de α nos dan debajo la pareja de χ_1.

Veamos que en α_2, también χ_2 contiene a `(d z)`. Visualmente, vemos que la pareja de α_2 `(p u)` nos da debajo la pareja `(d z)`.

```
α2 : abcdefghijklmnopqrstuvwxyz
     jwezchxfnamtkiquoyvlpsbgrd
13   jlukhfcnvoepwrxzsytqdimagb
```

.

Por tanto, χ_2 efectivamente contiene la permutación (d z).

Procediendo del mismo modo que antes, que la permutación α_1 contenga (l u) implica que (f r) forman parte de χ_1.

Mirando α_4, que (c q) sea una trasposición suya implica que (f r) forme parte de χ_4 y por tanto hay coincidencia.

Repitiendo los pasos anteriores con todas las α_i, el resultado es:

$$\begin{aligned}
\chi_1 &= \texttt{(au)(bv)(ci)(dz)(ek)(fr)(gy)(hl)(jm)(np)(ox)(qt)(sw)}\\
\chi_2 &= \texttt{(ac)(bk)(ti)(dz)(ew)(fn)(gy)(hu)(jo)(lm)(pq)(rv)(sx)}\\
\chi_3 &= \texttt{(am)(bl)(cz)(dx)(er)(fg)(ho)(in)(ju)(ky)(ps)(qt)(vw)}\\
\chi_4 &= \texttt{(ai)(bl)(cj)(dq)(ek)(fr)(gy)(ho)(ms)(nw)(pt)(ux)(vz)}\\
\chi_5 &= \texttt{(am)(bg)(ti)(dz)(ej)(fu)(sy)(hp)(wr)(cx)(ok)(ql)(nv)}\\
\chi_6 &= \texttt{(am)(bv)(ti)(do)(ez)(fr)(gj)(hs)(kp)(cx)(nw)(ql)(uy)}
\end{aligned}$$

La mayoría de las parejas no estarán en la χ desconocida. Vemos que hay varias repeticiones de trasposiciones en distintas χ_i: (am), (dz), (ti), (fr), (gy), por lo que es probable que aparezcan en χ.

Obviamente, χ_1 también se puede calcular sin la rejilla ya que tan solo es un método para calcularla más fácilmente. Es decir, calcular $\chi_1 = \nu_{12}^{-1}\alpha_1\nu_{12}$:

$$\nu_{12} = \pi^{12}\nu\pi^{-12} = \texttt{(acmq)(bkpy)(dvelfioszh)(jw)(nx)(rtu)}$$

Por tanto,

$$\nu_{12}^{-1} = \pi^{12}\nu^{-1}\pi^{-12} = \texttt{(aqmc)(bypk)(dhzsoiflev)(jw)(nx)(rut)}$$

Además, sabemos que $\alpha_1 = \texttt{(af)(bv)(cw)(dy)(ez)(gp)(sh)(in)(jo)(kx)(mr)(qt)(lu)}$.

Luego $\alpha_1^{\nu_{12}} = \texttt{(au)(bv)(ci)(dz)(ek)(fr)(gy)(hl)(jm)(np)(ox)(qt)(sw)} = \chi_1$, y por tanto α_1 conjugado con $\pi^{12}\nu\pi^{-12}$ es igual a χ_1.[2].

Uso de la rejilla para encontrar el rotor derecho y el ajuste conjunto

Una vez visto en el caso concreto en el que se coloca en la posición correcta, ¿cómo se encontraba esta posición?
Como hemos dicho en la introducción del método, la hoja superior, la cual contenía las permutaciones α_i, se desliza por todas las posibles posiciones del rotor ν y el criptoanalista busca consistencia con la permutación χ. Esta se consigue buscando el mayor número de trasposiciones repetidas en las diferentes χ_i (una por cada α_i). Este procedimiento se realizaba directamente sobre la hoja del rotor derecho si se conocía el orden de los rotores, pero si por el contrario se desconocía, había que repetirlo para cada uno de los tres rotores, buscando el que generaba más repeticiones.

[2]La conjugación se puede seguir procediendo igual que en el ejemplo 3.2

Se elegiría la posición $\pi^{12}\nu\pi^{-12}$ para α_1 por ser la posición con más repeticiones en las χ_i. Si la colocamos en otra posición hay una disminución notable en las repeticiones. Vemos que, si por ejemplo, colocamos α_1 en la 3 en vez de en la 12, ninguna trasposición se repite 3 veces. Calculamos las χ_i con la rejilla en la posición 3, obteniendo:

$$\chi_1 = \texttt{(ah)(bt)(cs)(dg)(fk)(ex)(jn)(iz)(lr)(my)(ov)(pw)(qu)}$$
$$\chi_2 = \texttt{(ac)(bm)(dn)(ei)(fx)(gj)(hs)(kq)(ly)(ow)(pv)(rz)(tu)}$$
$$\chi_3 = \texttt{(ao)(bk)(ce)(dt)(fx)(gr)(hq)(iz)(jl)(mw)(ns)(py)(uv)}$$
$$\chi_4 = \texttt{(as)(bc)(de)(fl)(gy)(hk)(io)(jr)(mz)(nw)(pv)(qx)(tu)}$$
$$\chi_5 = \texttt{(av)(bk)(cl)(ds)(er)(fg)(hy)(iw)(jt)(mn)(ox)(pu)(qz)}$$
$$\chi_6 = \texttt{(af)(bu)(cm)(dg)(hr)(ex)(il)(jq)(kw)(ns)(ot)(py)(vz)}$$

Uso de la rejilla para encontrar el clavijero

Una vez conocidos el rotor derecho y los ajustes exactos usados, veamos cómo se usa la rejilla para obtener el clavijero. Como hemos dicho antes, esta parte es la más complicada por ser la que más posibilidades tenía de configurarse. Volviendo a la posición correcta tenemos

$$\begin{aligned} \alpha_1 &= \sigma\nu_{12}\chi\nu_{12}^{-1}\sigma \\ \alpha_2 &= \sigma\nu_{13}\chi\nu_{13}^{-1}\sigma \\ &\vdots \end{aligned}$$

Si llamamos $\overline{\alpha_i} = \alpha_i^\sigma$, tenemos

$$\begin{aligned} \overline{\alpha_1} &= \alpha_1^\sigma = \nu_{12}\chi\nu_{12}^{-1} \\ \overline{\alpha_i} &= \alpha_2^\sigma = \nu_{13}\chi\nu_{13}^{-1} \\ &\vdots \\ \overline{\alpha_i} &= \alpha_i^\sigma = \nu_{11+i}\chi\nu_{11+i}^{-1} \end{aligned}$$

siendo $\nu_{11+i} = \pi^{11+i}\nu\pi^{-11-i}$.

No podemos calcular $\overline{\alpha_i}$ ya que no conocemos σ, pero como σ deja fijas 14 letras, algunas parejas de $\overline{\alpha_i}$ estarán en α_i (al menos las que tengan las dos letras fijas en el clavijero). Veamos qué ocurre con α_1.

Al aplicar ν_{12} a α_1 será lo mismo que aplicárselo a $\overline{\alpha_1}$ para esas parejas de letras que quedan fijas por el clavijero. Así

$$\alpha_1^{\nu_{12}} = \texttt{(ci)(ke)(mj)(vb)(lh)(gy)(zd)(ox)(ws)(pn)(qt)(fr)(au)}$$

Llamamos a esto χ_1. Como no conocemos $\overline{\alpha_1}$ no sabemos cuál es χ, pero sabemos que alguna trasposición de $\alpha_1^{\nu_{12}} = \chi_1$ también aparecerá en χ. Lo mismo ocurre con el resto de χ_i.

Como hemos dicho antes, las trasposiciones que se repiten en las χ_i es probable que estén en la χ real, precisamente porque son letras que provienen de parejas de α formadas por letras que quedan fijas por el clavijero. Por ello vamos a ir suponiendo que cada una de esas trasposiciones repetidas están en χ, y veamos si sacamos algo en claro del clavijero, o por el contrario, llegamos a contradicción.

.

Suponemos pues que (am) está en χ. Como $\overline{\alpha_i} = \nu_{11+i}\chi\nu_{11+i}^{-1}$, si conozco una pareja de χ, entonces conozco una pareja de $\overline{\alpha_i}$.
(am) aparece repetida en χ_3, χ_5, χ_6. Fijándonos en i = 3, si conjugamos (am) con ν_{14}^{-1} :

$$\begin{array}{rl} \alpha_3: & \texttt{abcdefghijklmnopqrstuvwxyz} \\ & \texttt{omhxpvyczqunblaejsrwkftdgi} \\ 14 & \texttt{ktjgebmundovqwyrxspchlzfai} \end{array}$$

Obtenemos pues (yg), que estará en $\overline{\alpha_3}$, y vemos que efectivamente está en α_3. Por tanto, si en α_3 está (yg) y en $\overline{\alpha_3}$ también, es bastante probable que g e y queden fijas por el clavijero.

χ	σ
(am)	(g) (y)

Pasamos a i=5 y conjugamos (am) con ν_{16}^{-1}, obteniendo (ri), que está en $\overline{\alpha_5}$ y en α_5. Por tanto, igual que antes, es bastante probable que σ deja r e i fijas.

Del mismo modo, con i=6, y conjugando con ν_{17}^{-1}, obtenemos que g y p probablemente queden fijas.

χ	σ
(am)	(g) (y) (r) (i) (p)

Pasamos ahora a analizar las χ_i en las que no se repite (am).

Para i=1, al conjugar (am) obtenemos que en $\overline{\alpha_1}$ está (cq), pero esta trasposición no está en α_1, luego las dos letras no pueden quedar fijas por σ. Por tanto, sabemos que al menos una de las dos letras se mueve por σ, pero no sabemos a qué pareja de α_i van. De momento no podemos sacar información de aquí, ya que ninguna de las letras nos han aparecido antes en el clavijero.

Lo mismo ocurre con i=2, con lo que obtenemos que en $\overline{\alpha_2}$ está (wx), pero esta trasposición no está en α_2. Y con i=3, obteniendo que en $\overline{\alpha_3}$ está (eh), pero esta trasposición no está en α_3. Tampoco podemos saber a qué pareja son movidas por σ.

Suponemos ahora que (ti) está en χ.

Con respecto a i=1, dicha pareja se transforma en (fr) mediante la conjugación, por lo que está en $\overline{\alpha_1}$. Esta pareja no está en α_1, luego, o f o r se mueven, pero ya nos ha salido antes que r está fija. Por tanto, la pareja (fr) irá a una pareja de α_1 de la forma (_r), es decir, (mr).

$$\begin{array}{rl} \alpha_1: & \texttt{abcdefghijklmnopqrstuvwxyz} \\ & \texttt{fvwyzapsnoxurijgtmhqlbckde} \end{array}$$

Así, vemos que σ intercambia (fm).

Para i=2, la trasposición obtenida que pasa a formar parte de $\overline{\alpha_2}$ es (sv), que también está en α_2, luego s y v están fijas por σ.

Para i=3, $\overline{\alpha_3}$ = (bz)..., pero no está en α_3, luego como antes, irá a una pareja de α_3, pero no sabemos a cuál, ya que de momento no sabemos nada de b ni z.

.

$\overline{\alpha_4}$ = (bg)..., y sabemos que g está fija, por tanto (bg) va a la trasposición de g que esté en α_4 : (lg). Y así, el clavijero mueve (bl).

Una vez sabemos qué pasa con b en el clavijero, podemos volver al caso anterior. Si sabemos que (bl) forman parte del clavijero, (bz) irá a la pareja de l que además esté en α_3, es decir, (ln). Por tanto, obtenemos que (zn) está en el clavijero.

$\overline{\alpha_5}$ = (jy)..., que está en α_5, luego j e y fijas por el clavijero.

$\overline{\alpha_6}$ = (ks)..., también pertenece a α_6, luego k y s están fijas en σ.

χ	σ
(am)	(g) (y) (r) (i) (p)
(ti)	(fm) (s) (v) (bl) (zn) (j) (y) (k)

Supongamos ahora que (dz) está en χ.

$\overline{\alpha_1}$ = (hs)..., que está en α_1, luego s y h están fijas por σ.

$\overline{\alpha_2}$ = (up)..., que también está en α_2, luego u y p están fijas por σ.

$\overline{\alpha_3}$ = (jw)..., pero no está en α_3, luego, o j o w se mueven, pero ya nos ha salido antes que j está fija. Por tanto, la pareja (jw) irá a una pareja de α_3 que tenga la j, es decir, (jq). Así, vemos que σ intercambia (wq).

$\overline{\alpha_4}$ = (dx)..., que no está en α_4, pero de momento no sabemos nada de d ni de x.

$\overline{\alpha_5}$ = (vd)..., que está en α_5, luego v y d fijas por el clavijero.

Una vez sabemos qué pasa con d en el clavijero, podemos volver al caso anterior. Si sabemos que (d) está fija en el clavijero, (dx) irá a la pareja de d que además esté en α_4, es decir, (do). Por tanto, obtenemos que (ox) está en el clavijero.

$\overline{\alpha_6}$ = (aq)..., que no está en α_6, pero sabemos que (qw) forma parte del clavijero, luego (aq) irá a parar a (ew) por el clavijero. Así, (ae) están en σ.

χ	σ
(am)	(g) (y) (r) (i) (p)
(ti)	(fm) (s) (v) (bl) (zn) (j) (y) (k)
(dz)	(h) (s) (u) (p) (wq) (v) (d) (ox) (ae)

Con los datos que tenemos, volvemos al caso en el que (am) está en χ:

(cq) $\longrightarrow$ (cw) $\Longrightarrow$ (c) fija.
(wx) $\longrightarrow$ (qo) $\Longrightarrow$ (ox) pertenecen al clavijero.

.

(eh) $\longrightarrow$ (ah), que pertenece a α_4, luego no hay contradicción en las trasposiciones obtenidas.

χ	σ
(am)	(g) (y) (r) (i) (p) (c) (ox) (h)
(ti)	(fm) (s) (v) (bl) (zn) (j) (y) (k)
(dz)	(h) (s) (u) (p) (wq) (v) (d) (ox) (ae)

Suponemos ahora que (fr) está en χ:

$\overline{\alpha_1}$ = (lu)..., que también pertenece a α_1, y por el mismo razonamiento usado anteriormente, l y u deberían estar fijas, pero esto contradice lo ya obtenido, ya que (bl) están en el σ.

Vemos que con el resto de $\overline{\alpha_i}$ también llegamos a contradicción:

$\overline{\alpha_2}$ = (fn)..., no está en α_2. Sabemos que una trasposición es (fm), luego (fn) iría a (mk), y por tanto, (nk) formarán parte de σ, pero esto contradice que k está fija.

$\overline{\alpha_3}$ = (xp)..., que por lo que sabemos, debería ir a (op), sin embargo, esta trasposición no está en α_3.

$\overline{\alpha_4}$ = (cq)..., que también está en α_4, lo que implicaría que ambas quedan fijas por el clavijero. Pero este hecho también contradice que (qw) estén en σ.

$\overline{\alpha_5}$ = (sz)..., y por lo que sabemos, iría a (sn). Vemos la contradicción ya que (sn) no está en α_5.

$\overline{\alpha_6}$ = (ew)..., que también está en α_6, lo que implicaría que ambas quedan fijas por el clavijero. Pero esto contradice que (qw) y (ae) estén en σ.

Vemos pues que la suposición de que (fr) está en χ no es cierta.

Suponemos por último que (gy) está en χ:

$\overline{\alpha_1}$ = (gp)..., que al estar también en α_1 implica que ambas son fijas.

$\overline{\alpha_2}$= (yr)..., que también pertenece a α_2, luego ambas son fijas.

$\overline{\alpha_3}$ = (do)..., pero esta trasposición no pertenece a α_3. Sin embargo, sabemos qué pasa con cada una de las dos letras, que por el clavijero van a (dx), y esta sí pertenece a α_3.

$\overline{\alpha_4}$ = (tv)..., que vemos que pertenece a α_4, y por tanto, ambas letras quedan fijas por σ.

$\overline{\alpha_5}$ = (xw)..., que no pertenece a α_5, pero sabemos qué pasa con cada una de las dos letras, que por el clavijero van a (oq), y esta sí pertenece a α_5.

.

$\overline{\alpha_6}$ = (cz)..., que no pertenece a α_6, pero por el clavijero van a (cn), y esta sí pertenece a α_6.

Luego al no llegar a ninguna contradicción con los datos sacados anteriormente, podemos aceptar la suposición.

χ	σ
(am)	(g) (y) (r) (i) (p) (c) (ox) (h)
(ti)	(fm) (s) (v) (bl) (zn) (j) (y) (k)
(dz)	(h) (s) (u) (p) (wq) (v) (d) (ox) (ae)
(gy)	(t)

Tenemos pues las 6 trasposiciones de las que constaba el clavijero:

$$\sigma = \texttt{(fm)(bl)(wq)(ae)(xo)(zn)}$$

Ahora, con ese clavijero y el rotor, podemos comprobar que efectivamente sale la misma χ usando cualquiera de las α_i.

Con la notación introducida anteriormente, $\chi = \nu_{11+i}^{-1}\overline{\alpha_i}\nu_{11+i}$. Calculamos pues, en primer lugar, $\overline{\alpha_i} = \alpha_i^{\sigma}$ puesto que ya conocemos el clavijero.

$$\overline{\alpha_1} = \texttt{(an)(bu)(cq)(dy)(em)(fr)(gp)(hs)(iz)(jx)(ko)(lv)(tw)}$$
$$\overline{\alpha_2} = \texttt{(ac)(bt)(dn)(ej)(fk)(go)(hm)(iz)(lq)(pu)(ry)(sv)(wx)}$$
$$\overline{\alpha_3} = \texttt{(ap)(bz)(ch)(do)(ex)(fl)(gy)(in)(jw)(ku)(mv)(qt)(rs)}$$
$$\overline{\alpha_4} = \texttt{(al)(bg)(cw)(dx)(eh)(fo)(in)(jp)(kz)(ms)(qu)(ry)(tv)}$$
$$\overline{\alpha_5} = \texttt{(ak)(bs)(cu)(dv)(ez)(fn)(gp)(ho)(ir)(jy)(lt)(mq)(wx)}$$
$$\overline{\alpha_6} = \texttt{(aq)(bl)(cz)(dn)(ef)(gp)(hy)(io)(jt)(ks)(mx)(rw)(uv)}$$

Con esto podemos calcular χ para cada $\overline{\alpha_i}$ y ver si sale la misma para cada i:

$$i=1: \chi = \nu_{12}^{-1}\overline{\alpha_1}\nu_{12} = \texttt{(am)(bv)(cx)(dz)(ef)(gy)(ho)(it)(ju)(kr)(lq)(nw)(ps)}$$
$$i=2: \chi = \nu_{13}^{-1}\overline{\alpha_2}\nu_{13} = \texttt{(am)(bv)(cx)(dz)(ef)(gy)(ho)(it)(ju)(kr)(lq)(nw)(ps)}$$
$$i=3: \chi = \nu_{14}^{-1}\overline{\alpha_3}\nu_{14} = \texttt{(am)(bv)(cx)(dz)(ef)(gy)(ho)(it)(ju)(kr)(lq)(nw)(ps)}$$
$$i=4: \chi = \nu_{15}^{-1}\overline{\alpha_4}\nu_{15} = \texttt{(am)(bv)(cx)(dz)(ef)(gy)(ho)(it)(ju)(kr)(lq)(nw)(ps)}$$
$$i=5: \chi = \nu_{16}^{-1}\overline{\alpha_5}\nu_{16} = \texttt{(am)(bv)(cx)(dz)(ef)(gy)(ho)(it)(ju)(kr)(lq)(nw)(ps)}$$
$$i=6: \chi = \nu_{17}^{-1}\overline{\alpha_6}\nu_{17} = \texttt{(am)(bv)(cx)(dz)(ef)(gy)(ho)(it)(ju)(kr)(lq)(nw)(ps)}$$

Vemos pues que el clavijero es correcto.

A principios de la década de 1930, el orden de los rotores fue el mismo durante un mes o más, por lo que los polacos generalmente sabían qué rotor estaba en la posición más a la derecha y sólo necesitaban usar una hoja inferior. A finales de 1936, el orden de los rotores cambiaba todos los días. Los polacos necesitaban conocer primero de todo qué rotor ocupaba la posición derecha, por lo que desarrollaron el método del reloj basándose fundamentalmente en las características propias del lenguaje alemán. Con el uso de este método solo necesitarían examinar la hoja inferior de la rejilla del rotor derecho resultante del método.

.

Capítulo 5

Ciclómetro

En octubre de 1936, el número de pares de letras modificadas en el clavijero pasó de ser 6 a un número entre 5 y 8, lo que complicó el uso del método de la rejilla, por lo que tuvieron que buscar otro método para encontrar los ajustes. Centraron su atención en la relación que tenían las letras de los indicadores de los mensajes, esto es, la 1ª con la 4ª, la 2ª con la 5ª, y la 3ª con la 6ª. Rejewski llegó a la conclusión de que estas permutaciones eran una consecuencia directa de la configuración y disposición de los rotores, y que, aunque las conexiones del clavijero cambiasen, este hecho no provocaba una modificación en la estructura cíclica de estas. Esto es, el clavijero influía únicamente en el intercambio de las letras, por lo que el número de ciclos y sus longitudes dependían exclusivamente del orden de los rotores y de sus posiciones iniciales. Dicho número de ciclos y longitudes es lo que hemos denominado tipo en el Capítulo 3.

Veamos con permutaciones lo explicado anteriormente. De la ecuación 3.2, con ajuste conjunto c genérico, escribimos

$$\alpha_1\alpha_4 = \sigma\,\pi^{c+1}\,\nu\,\pi^{-c-1}\,\chi\,\pi^{c+1}\,\nu^{-1}\,\pi^{-c-1}\,\sigma\,\sigma\,\pi^{c+4}\,\nu\,\pi^{-c-4}\,\chi\,\pi^{c+4}\,\nu^{-1}\,\pi^{-c-4}\,\sigma =$$

$$= \sigma\,\pi^{c+1}\,\nu\,\pi^{-c-1}\,\chi\,\pi^{c+1}\,\nu^{-1}\,\pi^{3}\,\nu\,\pi^{-c-4}\,\chi\,\pi^{c+4}\,\nu^{-1}\,\pi^{-c-4}\,\sigma \tag{5.1}$$

ya que sabemos que σ tiene orden 2. Análogamente con $\alpha_2\alpha_5$ y $\alpha_3\alpha_6$. De estas ecuaciones, la parte central (sin σ) depende del orden de los rotores y del ajuste conjunto, no de las posiciones iniciales. Esta parte central vemos que es

$$\sigma\,\alpha_1\,\alpha_4\,\sigma = \overline{\alpha_1\alpha_4}$$

ya que en el capítulo anterior hemos definido $\overline{\alpha} = \alpha^{\sigma}$. Conociendo el ajuste conjunto (abc) eran capaces de calcular esta parte central. Lo que hicieron fue calcular dichas permutaciones para cada orden de los rotores y cada posición inicial de estos, teniendo un total de 26·26·26·6 = 105456 permutaciones, ya que, como hemos dicho, α y $\overline{\alpha}$ tienen la misma estructura de ciclos debido a que son conjugadas por el clavijero. Una vez calculadas hicieron un catálogo con sus tipos, indicando de qué orden de los rotores y posición inicial procedían.

Hacer ese cálculo a mano o con una máquina Enigma era muy largo y costoso, por tanto, si conseguían inventar una máquina que produjera la longitud de los ciclos para $\overline{\alpha_1\alpha_4}$, serían capaces de hacer una lista de los tipos para dichas expresiones en un tiempo reducido. Construyeron dicho aparato y lo llamaron ciclómetro. Una vez que se tenía el catálogo de los tipos de los productos de $\overline{\alpha}$, si para un día se conocían las α, serían capaces de conocer el orden de los rotores y los ajustes conjuntos utilizados ese día comparando con el catálogo.

Figura 5.1: Ciclómetro

El ciclómetro era una máquina Enigma doble (6 rotores y dos reflectores, en lugar de 3 y 1 respectivamente) pero en la que el rotor derecho del segundo juego de rotores estaba desplazado tres posiciones con respecto al rotor derecho del primer conjunto, mientras que los rotores central e izquierdo estaban posicionados de la misma forma en ambos conjuntos. En la imagen 5.1 puede verse su apariencia, donde podemos distinguir los dos grupos de rotores.

Como explica Rejewski en sus memorias [1], cuando se pulsaba el interruptor de una tecla, no solo se encendía la lámpara correspondiente a esa letra, sino todas las lámparas pertenecientes al mismo ciclo. Pulsando otro interruptor de una tecla no iluminada, otras teclas se iluminan. Dichas teclas determinaban otro ciclo. Así se obtenía la descomposición en ciclos disjuntos de $\overline{\alpha_1\alpha_4}$. Variando el orden de los rotores y de sus posiciones iniciales se obtienen todas las permutaciones $\overline{\alpha_1\alpha_4}$. Esto fue suficiente para calcular todos los tipos, ya que las permutaciones $\overline{\alpha_2\alpha_5}$ y $\overline{\alpha_3\alpha_6}$ asociadas a una determinada posición de los rotores coinciden con la $\overline{\alpha_1\alpha_4}$ obtenida tras adelantar los rotores de la derecha del ciclómetro una o dos posiciones, respectivamente.

Rejewski conocía los tipos de todas las permutaciones $\overline{\alpha_1\alpha_4}, \overline{\alpha_2\alpha_5}, \overline{\alpha_3\alpha_6}$ ya que podía calcular la parte central de la ecuación 5.1 para cada ajuste conjunto y orden de los rotores gracias al ciclómetro. Como $\overline{\alpha_i} = \sigma\alpha_i\sigma$ y sabemos que el clavijero no influye en el tipo, entonces comparando el tipo de las permutaciones obtenidas gracias al ciclómetro con los tipos de los productos de las α_i que conocían cada día, podían saber el ajuste conjunto y orden de los rotores utilizado.

La permutación σ se obtenía comparando las letras de los ciclos de las permutaciones $\alpha_1\alpha_4, \alpha_2\alpha_5$ y $\alpha_3\alpha_6$ con las de su correspondiente $\overline{\alpha_1\alpha_4}, \overline{\alpha_2\alpha_5}$ y $\overline{\alpha_3\alpha_6}$ obtenidos con el ciclómetro.

Females

Los alemanes introdujeron nuevos cambios en la configuración de la máquina Enigma. Estas variaciones hicieron que los métodos usados hasta entonces quedaran inservibles. Ya no había productos $\overline{\alpha_1\alpha_4}, \overline{\alpha_2\alpha_5}, \overline{\alpha_3\alpha_6}$ característicos cada día cuya configuración pudiera leerse en el catálogo ya que las α_i cambiaban en cada mensaje. Sin embargo, seguían repitiendo la clave del mensaje al inicio de cada comunicación. Ahora la cabecera del mensaje estaba formada por 9 letras: las tres primeras correspondientes al ajuste externo de los rotores, y las 6 siguientes resultaban del doble cifrado de la clave del mensaje. El resto del proceso del cifrado no sufrió variaciones. Una vez calculados los productos, comprobaron que el 40 % de estas permutaciones contenían ciclos de longitud 1. Esto es que en el conjunto de las 6 letras de los indicadores se producían repeticiones de letras en las posiciones 1-4, 2-5 ó 3-6. A

estas repeticiones se las llamó *females*. Veamos un ejemplo:

Ejemplo 5.1. Con una cantidad suficiente de material cifrado, se podían encontrar los siguientes indicadores:[1]

```
rtj  wahwik
hpn  rawktw
dqy  dwjmwr
```

Vemos que se repiten la 1ª y la 4ª, la 3ª y la 6ª, y la 2ª y la 5ª respectivamente. Fijándonos en el primer indicador, esto es que α_1 aplicado a una letra, digamos `x`, es `w`, y lo mismo con α_4. Por tanto tenemos α_1`(x) = w` y α_4`(x) = w`. Pero sabemos que Enigma tenía la propiedad de que si al pulsar una letra se iluminaba otra, al pulsar esa otra, se iluminaba la primera. Por tanto, α_4`(w) = x`, y si sustituimos esto en la otra igualdad tenemos $\alpha_1(\alpha_4$`(w)) = w`. Luego la permutación $\alpha_1\alpha_4$ tiene el ciclo `(w)`. Lo mismo ocurre con $\alpha_2\alpha_5$ y $\alpha_3\alpha_6$. Estas repeticiones se denotan 1,4-female, 2,5-female y 3,6-female, respectivamente.

Recordemos que las conexiones del clavijero no tenían ninguna influencia en las longitudes de $\alpha_1\alpha_4$, $\alpha_2\alpha_5$ y $\alpha_3\alpha_6$, ya que estas sólo dependen del orden de los rotores y de sus posiciones iniciales, viniendo determinadas por el ajuste conjunto. Por un lado, el ajuste externo era conocido, sin embargo, el interno era desconocido, aunque el mismo en todos los mensajes de un mismo día. Por tanto el ajuste conjunto era desconocido. Si se conseguía el ajuste conjunto, se podría saber el ajuste interno.

El objetivo pues era identificar el orden de cada rotor y la configuración del rotor de entre las 105456 posibles. Pero este factor se redujo en un factor 0'4 cada vez que aparecía un ciclo de longitud 1, ya que sólo el 40 % de las permutaciones tienen ciclos de este tipo.

En septiembre de 1938, Zygalski inventó un método adicional al desarrollado por Rejewski que determinaba el orden de los rotores y el ajuste interno, llamado las Hojas de Zygalski. Dicho método se basaba en la repetición de females.

Los cambios sucesivos realizados en la máquina Enigma por parte de los alemanes significó desarrollar varios métodos que permitieran desentrañar el código de Enigma de la mejor manera posible. Además de los métodos ya nombrados, hubo otros como el método del reloj de Ròzycki o el método ANX. Con la ayuda de unas invenciones basadas en réplicas de Enigma, Rejewski fue capaz de encontrar la clave del día de las comunicaciones alemanas antes de que acabara el día. Dichas invenciones fueron los aparatos electro-mecánicos llamados bombas, cuyo principal objetivo era mecanizar el sistema de catalogación para facilitar el conocimiento de las posiciones correctas de los rotores.

Una vez que tenían la clave del día, poseían la misma información que el receptor a quien iba dirigido el mensaje, y por tanto, podían descifrar el mensaje con la misma facilidad.

[1] Extraído de [1]

Bibliografía

[1] REJEWSKI, M. (1981), *How polish mathematicians deciphered the Enigma, Annals of the History of Computing 3(3): 213-234.*

[2] GALLARDO GÓMEZ, ROCÍO (2016), *El ataque polaco al protocolo ENIGMA* (Trabajo de Fin de Grado, Universidad de Sevilla).

[3] VÁZQUEZ, MANUEL , JIMÉNEZ-SERAL, PAZ (2018), *Recovering the military Enigma using permutations - filling in the details of Rejewski's solution.*

[4] VÁZQUEZ LAPUENTE, MANUEL, *Un matemático y enigmático recorrido desde Cambridge hasta Jaca.*

[5] JOSÉ MANUEL SÁNCHEZ MUÑOZ (2013), *Historias de Matemáticas. Criptología Nazi. Los Códigos Secretos de Hitler*,

[6] JOSÉ MANUEL SÁNCHEZ MUÑOZ (2013), *Descifrando Enigma. La Epopeya polaca*,

[7] ROTMAN, J. J. (1973), *The theory of groups. An introduction, Boston: Allyn and Bacon*,

[8] CHRISTENSEN, C. (2004) *Polish mathematicians finding patterns in Enigma messages, Mathematics Magazine,*

[9] HTTPS://WWW.CRYPTOMUSEUM.COM/

[10] HTTPS://EN.WIKIPEDIA.ORG/WIKI/GRILL_(CRYPTOLOGY) *Grill (cryptology)*