UNIVERSIDAD DE SEVILLA

FACULTAD DE MATEMÁTICAS

TRABAJO FIN DE GRADO

El ataque polaco al protocolo ENIGMA

PRESENTADO POR:

Rocío Gallardo Gómez

DIRIGIDO POR:

José María Tornero Sánchez

Sevilla, 2016

Índice general

Resumen

El principal objetivo de nuestro trabajo será desvelar las claves del exitoso ataque polaco al protocolo Enigma protagonizado por Marian Rejewski. Para ello, detallaremos el contexto histórico en el que se produjo dicho ataque, así como iremos desarrollando los diferentes métodos y técnicas que resultaron claves para la consecución de tal hito matemático. Comenzaremos describiendo el modelo Enigma atacado por los polacos, dando todo tipo de detalles tanto de la estructura física de la máquina, como del funcionamiento de la misma y el procedimiento de cifrado. Posteriormente, llevaremos a cabo una escrupulosa explicación sobre los resultados matemáticos necesarios para el ataque, basados en la teoría de permutaciones. Seguidamente, ilustraremos el procedimiento que siguió Rejewski para efectuar la desencriptación. Y, por último, desarrollaremos el ataque, propiamente dicho, exponiendo todos los métodos criptológicos, tanto manuales como mecánicos, que inventaron los polacos.

Palabras clave: criptografía, Enigma, Rejewski, permutaciones.

Abstract

The aim of our work will be to unveil the keys of the successful Polish attack to the Enigma protocol led by Marian Rejewski. In order to do so, we are going to introduce the historical context in which that attack was performed, while we develop the different methods and techniques that were vital for the success of such a mathematical milestone. After that, we will proceed to a detailed explanation of the mathematical results needed for the attack, based on permutation theory. Then, we are going to depict the procedure followed by Rejewski to carry out the decyphering. And, finally, we will describe the attack itself, expounding every cryptological method, manual and mechanical ones, that were created by the Polish cryptographers.

Keywords: cryptography, Enigma, Rejewski, permutations.

Capítulo 1

Introducción histórica

El origen de la criptografía[1] se remonta a miles de años. Históricamente ha estado vinculada a la protección de la confidencialidad de informaciones militares y políticas, lo que conlleva la necesidad de buscar métodos que rompan dicha protección, difícil tarea, más aún sin conocimientos matemáticos.

A principios del siglo XX, la invención de máquinas mecánicas y electromecánicas complejas, como la máquina de rotores Enigma, proporcionaron métodos de cifrado más sofisticados y eficientes. Así nace la criptología[2] científica, iniciada en 1949.

En época de guerra se hace indispensable que en el caso de que el enemigo intercepte nuestros mensajes, no tenga manera de saber qué significan. Con el paso del tiempo, la criptografía se convirtió en una pieza clave dentro de los ejércitos de todo el mundo.

1.1. Evolución de la criptología

Desde las más sencillas técnicas de encriptación, como el *Cifrado de César*, hasta las más modernas basadas en sofisticados algoritmos matemáticos manejados por potentes ordenadores, un sinfín de métodos de cifrado se han sucedido en la historia. Algunos ejemplos de ello son[3]:

- ***Escítala espartana*:** Bastón en el cual se enrollaba en espiral una tira de cuero donde se escribía el mensaje en columnas paralelas al eje del palo. Podía leerse volviendo a enrollar la tira sobre un palo del mismo

[1] Arte y técnica de escribir con procedimientos o claves secretas o de un modo enigmático, de tal forma que lo escrito solamente sea inteligible para quien sepa descifrarlo. Proviene del griego *kryptos* que significa oculto, y *graphia*, que significa escritura.

[2] Disciplina científica que se dedica al estudio de la escritura secreta, es decir, estudia los mensajes que, procesados de cierta manera, se convierten en difíciles o imposibles de leer por entidades no autorizadas. Proviene del griego *krypto*, y *logos*, que significa palabra.

[3] Podemos encontrar más detalles y ejemplos en [3].

diámetro que el primero. Usado en la guerra entre Atenas y Esparta en el siglo V a.C.

- ***Cifrado de César*:** Consiste en reemplazar cada letra del mensaje por la letra correspondiente tres posiciones más allá en el abecedario. Utilizado por Julio César en *La guerra de las Galias* (siglo I a.C.).
- ***Disco de Alberti*:** Constituye el primer cifrado por sustitución polialfabético conocido. Descrito en 1466 por Leon Battista Alberti, conocido como el padre de la Criptología Occidental.
- ***Cifra Vigenère*:** Consiste en una disposición de letras que contiene en orden los 26 alfabetos de César. Inventada por Blaise Vigenère en el siglo XVI.

Aunque la criptología ha usado durante mucho tiempo métodos matemáticos, fue sólo a partir de 1920, con la introducción de las máquinas de cifrado, cuando la aplicación de las matemáticas a la criptología tuvo una gran expansión.

1.2. El origen de Enigma

El período donde tomó una vital importancia fue en la Segunda Guerra Mundial, en la que el cifrado y el descifrado de códigos se convirtió en otro frente más de lucha. Ello fue debido a la aparición de un sistema de cifrado usado por Alemania, uno de los inventos más fascinantes de esa época, la máquina **Enigma**.

En 1923, tras el fracaso de Alemania en la Primera Guerra Mundial, todo el que tuviera dinero había quedado arruinado. Sin embargo, por fin la inflación desapareció, el panorama político se estabilizó y la economía empezó a crecer.

Una de las personas que en 1923 decidió montar un negocio fue un ingeniero alemán llamado Arthur Scherbius, el cual se asoció con otro ingeniero, Richard Ritter, para poner en marcha un nuevo invento que parecía que revolucionaría el arte de la criptografía. Otros inventores habían desarrollado el mismo concepto con meses de diferencia, entre los que se encontraba el holandés Hugo Alexander Koch. Scherbius y Ritter compraron la patente a Koch y construyeron una empresa llamada *Chiffriermaschinen Aktien Gesellschaft* (ChiMaAG) que comercializaría, bajo la marca Enigma, una máquina de cifrar aparentemente invencible.

Aunque la compañía, con el nombre que se le conoce, fue fundada en 1923, Scherbius solicitó la primera patente de la máquina Enigma comercial el 23 de febrero de 1918. Pese a que parecía un gran invento, su desorbitado precio

(equivalente a 30000 euros actuales) la convirtió en un gran fracaso. No obstante, la compañía lanzó varios modelos, cada uno de los cuales mejoraba el anterior. Con el modelo C, se quiso dar al mercado un producto más compacto y económico.

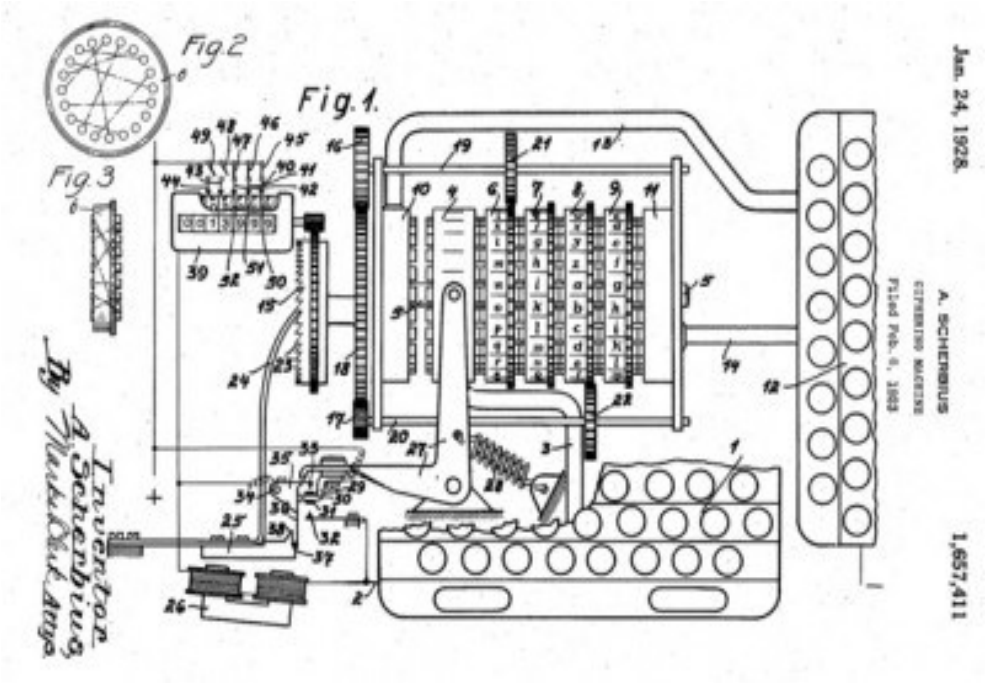


Figura 1.1: Patente americana de Enigma.

Antes de montar la empresa, Scherbius había ofrecido su invento a la Marina alemana y al Ministerio de Asuntos Exteriores y ambos le hicieron saber que, aunque parecía muy seguro, no tenían un tráfico que justificara su alto coste. Sin embargo, cuando en 1925 el gobierno italiano la adoptó oficialmente para su Marina, el Ejército alemán recapacitó y envió oficiales de inteligencia para evaluar Enigma, retomando el proyecto y confiándolo a la división de cifrado del Ministerio de Guerra alemán (*Chiffrierstelle*).

Con el lanzamiento del modelo Enigma-D obtuvieron verdadero éxito comercial. Pese al origen comercial de Enigma, la Armada alemana en febrero de 1926, y posteriormente el Ejército (*Wehrmacht*) el 15 de junio de 1928, adquirieron su propia máquina Enigma, adaptándola y cambiando su fisonomía acorde a sus necesidades y con el fin de aumentar el número de posibilidades de cifrado, complicando más aún si cabe su criptoanálisis.

1.3. El origen del ataque

Tras la Primera Guerra Mundial, los aliados se encargaron de vigilar las comunicaciones germanas. En 1926 comenzaron a tener problemas, ya que empezaron a interceptar mensajes cifrados con un nuevo método desconocido hasta el momento. En mitad de esta confusión se hallaba el recientemente formado estado de Polonia, rodeado de estados hambrientos por expandirse.

Los oficiales de inteligencia de los países que vigilaban Alemania pasaron informes muy pesimistas sobre la posibilidad de criptoanalizar los mensajes cifrados con Enigma. Si aquella máquina se vendía por todo el mundo, los días del criptoanálisis estarían contados.

Debido al clima de desconfianza que se generó, en enero de 1929, el director de la Universidad de Poznań preparó una lista de 20 estudiantes de matemáticas de últimos cursos que recibieron un llamamiento del ejército para participar en un curso de criptología. Las clases se impartirían durante dos noches a la semana en dicha Universidad y para ello debieron jurar mantener toda la operación en secreto.

Transcurridas varias semanas, muchos de los estudiantes que comenzaron el curso fueron abandonando por diversas razones. Únicamente tres de los estudiantes fueron capaces de compaginar sus estudios con el curso, Marian Rejewski, Jerzy Różycki y Henryk Zygalski.

Por otra parte, los polacos crearon en 1931 el *Biuro Szyfrów* (Oficina de Cifras) cuya tarea se basó en el intento de desencriptar los mensajes cifrados alemanes. Una vez creada dicha oficina, se formó un grupo de trabajo, dirigido por el capitán Maksymilian Ciężki, que llegó a una conclusión sorprendente: los alemanes habían abandonado el cifrado mediante códigos tradicionales y habían empezado a utilizar algún tipo de encriptación polialfabética mecánica. Siendo Enigma alemana, las sospechas se inclinaban a que estuvieran utilizando esta. Así, el grupo organizó un operativo y consiguió adquirir de forma encubierta una Enigma-D. Desmontaron la máquina y concluyeron que, incluso siendo esa misma la máquina usada por los militares alemanes, no había forma de descifrar los mensajes. Polonia estaba ahora inerme.

Las buenas noticias no tardaron en llegar. En 1930, un individuo que trabajaba en la Oficina de Cifra alemana, Hans Tilo Schmidt[4], contactó con la embajada francesa[5] en Berlín para ofrecer secretos a cambio de dinero. Puso a disposición de los franceses manuales de operación de Enigma pertenecientes a la Aviación y al Ejército de tierra, dos de los cuales describían sistemáticamente los pasos sucesivos del procedimiento de cifrado. Además Schmidt les

[4]Su nombre en clave fue *Asché* (pronunciación francesa de la H).

[5]El departamento de criptoanálisis francés, al igual que el polaco, también había topado con Enigma.

entregó unos carretes en los que había fotografías detalladas de la máquina Enigma usada por los alemanes. Sin embargo, los técnicos franceses llegaron a la conclusión de que esto no servía para nada. Era interesante saber cómo se operaba la máquina, pero ello no ayudaba a descifrarla. De este modo, los criptoanalistas franceses fueron incapaces de sacar partido de dicha información.

En virtud del tratado de colaboración que franceses y polacos habían firmado tras la Primera 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 los polacos. Esto significó un punto de inflexión en el ataque al código Enigma.

Dado que la máquina se había instaurado de forma total en el Ejército alemán, conllevando esto la necesidad de profesionalizar las tareas criptológicas de los estudiantes polacos, el puesto de Poznań fue cerrado en verano de 1932, por lo que Rejewski, Różycki y Zygalski comenzaron a formar parte del Biuro Szyfrów en Varsovia. De esta manera nacía el $BS4$ y comenzaba la guerra contra Enigma.

1.4. El principio del fin de Enigma

A pesar de la cantidad de personas encargadas en la desencriptación del código, una de las más influyentes fue Rejewski. Desde su reclutamiento en 1929 había estado rompiendo códigos menores de la Marina alemana con insultante facilidad. Él había sentido el racismo de los alemanes hacia los polacos en su propia carne, por lo que estaba listo a consagrar su vida a la lucha secreta contra aquella pesadilla que el destino había cruzado en el futuro de su nación.

Todo lo relacionado con Enigma se guardaba en una sola habitación bajo llave, cuyo acceso estaba fuertemente restringido. Rejewski pasó muchas horas pensando solo en aquella habitación, rodeado de los manuales, los libros de claves y docenas de carpetas rotuladas como *Top Secret*. Mediante permutaciones, construyó el modelo matemático de una máquina Enigma. Finalmente, Rejewski supo por dónde empezar, aunque no a dónde llegaría.

La guerra criptológica

Con la ayuda de los demás criptoanalistas, realizó una hazaña criptográfica sin precedentes, al conseguir en apenas un mes el secreto del cableado de la máquina, la gran incógnita. Tras unos días de reflexión, el equipo de criptoanalistas, reforzado por aquel extraordinario genio, halló una vía para obtener las posiciones iniciales de Enigma para cada mes.

La tarea que se le presentó a Rejewski resultó ser demasiado enorme y complicada, por lo que terminó pidiendo ayuda a sus compañeros de curso, Ròżycki y Zygalski. Conjuntamente, diseñaron el ciclómetro, el cual se trataba de una máquina Enigma doble de la que daremos detalles más adelante. Así, armados con varios ciclómetros, el equipo de Rejewski procedió a crear una enciclopedia a base de teclear todas las combinaciones para todas las posiciones de la máquina. Tardaron casi un año, pero cuando terminaron en 1933 era trivial encontrar la clave del día. Ahora el problema ya no era descifrar, sino manejar y clasificar aquella ingente cantidad de información.

En noviembre de 1937 los alemanes hicieron su primer movimiento desde la creación de la Enigma militar. Sin embargo, este cambio solo supuso una molestia pasajera para Rejewski. Más tarde, concretamente el 15 de septiembre de 1938, las secciones de cifra de todas las unidades del ejército alemán empezaron a usar un nuevo procedimiento. Aunque nunca volvería a ser tan fácil como había sido antes de septiembre, pronto volvería a ser posible descifrar los mensajes masivamente.

En septiembre de ese mismo año, Zygalski inventó un ingenioso método en pocos días. Este invento, que se conoce como método de las *hojas de Zygalski* o *Netz*[6] era rudimentario aunque bastante efectivo. Una vez aplicado, la máquina Enigma volvía a estar tan indefensa como antes del cambio de procedimiento, salvo que ahora a costa de más trabajo diario que antes.

Por otro lado, también Ròżycki contribuyó en gran medida a la lucha contra Enigma desarrollando el denominado *método del reloj*, el cual sería perfeccionado más tarde.

Después de casi siete años de contacto directo con Enigma, los matemáticos polacos estaban completamente lanzados. Mientras Zygalski y Ròżycki trabajaban en sus diseños, Rejewski presentó los planos de un nuevo aparato que había inventado: la *bomba criptológica*. Se trataba de unos aparatos electro-mecánicos basados en la combinación de 6 réplicas de la Enigma polaca construida previamente. Es el primer caso conocido de prueba de fuerza bruta mecanizada, aunque muchas veces requería algunas pruebas manuales posteriores.

A finales de diciembre de 1938, muchas redes de operadores de radio alemanes empezaron a usar la máquina con nuevas modificaciones. Aunque los matemáticos sabían cómo seguir, el cambio era difícilmente asumible, por temas logísticos y de presupuesto. Por primera vez cundió el desánimo entre los criptógrafos polacos.

La permisividad para con el régimen nazi y la presión que aquellos ejercieron sobre el gobierno polaco, con el fin de permitir la anexión de Danzig,

[6]Proviene del alemán *Netzverfahren*, que significa método neto.

crearon el caldo de cultivo para la invasión alemana de Polonia. Después de sólo veinte años, Polonia estaba a punto de dejar de existir otra vez. Bajo esta amenaza, los polacos decidieron que era necesario informar de sus avances criptoanalíticos, con el fin de que estos no se perdieran.

La búsqueda de aliados

Polonia preveía que pronto dejaría de beneficiarse del trabajo de Rejewski, por lo que quiso que al menos los aliados tuvieran la oportunidad de tratar de usarlo para seguir avanzando. Así, el 9 de enero de 1939 se organizó una infructuosa reunión en París entre criptólogos polacos, franceses y británicos.

Finalmente, a mediados de julio de 1939, cuando la invasión alemana de Polonia parecía inminente, el general del ejército polaco autorizó al Biuro Szyfrów a compartir con los aliados todos los conocimientos técnicos sobre el descifrado de Enigma.

El 24 de julio de ese mismo año, el jefe de los criptoanalistas británicos de la Oficina Exterior (*Foreign Office*) organizó una reunión en un viejo búnker, situado en los bosques de Kabackie, cerca de Varsovia, a la que asistieron británicos y franceses. Este búnker resultó ser el centro neurálgico del ataque polaco al código Enigma. Uno de los integrantes del equipo británico que se reunió fue el jefe de las operaciones criptográficas de Bletchley Park, el comandante Alastair Denniston, un reconocido defensor de la importancia de las matemáticas en la lucha criptoanalítica.

Bletchley Park

Bletchley Park era la sede del *Government Code & Cypher School (GC&CS)*[7], una organización de descodificación fundada en Buckinghamshire que, tras el estallido de la guerra, se convirtió en la sede clandestina y secreta del ataque a Enigma, donde trabajaron alrededor de 12000 personas a lo largo de la guerra[8].

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.

El posterior gran éxito de Bletchley Park se debe a la apuesta de Denniston de incluir en esta lucha a las mejores mentes matemáticas del momento en Gran Bretaña, entre los que se encontraba Alan Turing, genio matemático del King's College de Cambridge.

[7]Escuela Gubernamental de Códigos y Cifras.

[8]Curiosamente, un alto porcentaje de esas personas fueron mujeres.

Alan Turing

La criptografía de ese tiempo desconfiaba de los matemáticos y, recíprocamente, estos la consideraban un arte menor, pero Turing, después de haber visitado los más áridos altiplanos de la teoría matemática, bien podía rebajarse un poco por Inglaterra. Así que decidió aceptar la oportunidad de ayudar a su país y con ello dio un paso que le otorgaría una inesperada gloria militar, pero también le llevaría al infierno personal más terrible.

Su técnica consistió en buscar lo que en criptología se denominan *puntales*[9]. Además, fue capaz de construir un modelo mejorado de la bomba polaca, al que denominó *bombe*.

La combinación de los estudios polacos junto con las técnicas halladas por los aliados resultó ser finalmente una estrategia extraordinaria de criptoanálisis, capaz únicamente de ser planificada por una mente privilegiada como la de Turing.

1.5. Unos héroes olvidados

Tras la invasión germana de Polonia, una gran cantidad del $BS4$ fueron capturados, torturados y asesinados. Afortunadamente, Rejewski, Zygalski y Ròżycki pudieron abandonar el país a tiempo y pusieron rumbo a Rumanía. No obstante, lejos de querer abandonar su carrera, estos decidieron seguir con su guerra criptológica en el centro de inteligencia franco-polaca[10].

La unidad *Bruno* se vio obligada a evacuar tras la amenaza de invasión de Alemania, por lo que nuestros protagonistas tuvieron que volver a huir, poniendo rumbo a Argel. Sin embargo, tras la rendición francesa, los integrantes de esta unidad decidieron crear una nueva unidad encubierta denominada *Cadix*.

Debido al cúmulo de amenazas y con el fin de evitar sospechas, Rejewski decidió emplearse como profesor de matemáticas en Nantes.

Varios problemas surgieron de nuevo. Varios criptológos pertenecientes a *Cadix* tuvieron que realizar un viaje a Argel. Cuando volvían de este, el barco donde viajaban naufragó. Entre los 301 pasajeros que perdieron la vida se encontraron varios criptólogos fundamentales en el trabajo contra el código Enigma, desgraciadamente uno de ellos fue Jerzy Ròżycki.

Los alemanes volvieron a descubrir las operaciones secretas de los criptoanalistas, por lo que los miembros de *Cadix* tuvieron que huir de nuevo. Así,

[9] *Cribs* en inglés.

[10] A este centro se le denominó *Bruno*.

Rejewski y Zygalski pusieron rumbo a España, con el infortunio de ser descubiertos tras cruzar los Pirineos. Tras esto, fueron arrestados y encarcelados. Sin embargo, pronto fueron liberados y enviados a Madrid.

Cuando parecía que había llegado la tranquilidad a nuestros personajes, estos se vieron sucumbidos por la traición de un oficial de la inteligencia militar francesa. De este modo, fueron nuevamente capturados y enviados a un campo de concentración alemán.

Tras el fin de la guerra, Rejewski regresó a Polonia y comenzó a trabajar como contable, Zygalski permaneció exiliado en el Reino Unido donde trabajó como profesor de estadística matemática en la Universidad de Surrey, y Turing, tras ser sometido a la castración química por ser homosexual, decidió quitarse la vida.

Este fue el indecente, inmoral y deshonesto reconocimiento recibido por estos matemáticos que, convertidos prácticamente en soldados, decidieron consagrar su vida en la lucha contra Enigma.

Capítulo 2

Descripción del modelo Enigma atacado por los polacos

Como hemos visto en el capítulo anterior, la máquina Enigma fue el código secreto utilizado por el ejército alemán para sus comunicaciones en la Segunda Guerra Mundial. Dicha máquina disponía de un mecanismo de cifrado rotatorio, que permitía usarla tanto para cifrar como para descifrar mensajes. Realmente era una evolución de otros modelos electromecánicos que intentaba hacer más sencilla y automatizada la tediosa tarea de encriptar y desencriptar mensajes. Su amplio uso se debe a su facilidad de manejo y supuesta inviolabilidad.

2.1. Estructura física de la máquina

Enigma era muy similar a una máquina de escribir[1], con la salvedad de que se alimentaba de una batería y no empleaba papel. Aunque la máquina disponía de dicha batería, también podía usar la energía eléctrica si estaba disponible. Al igual que las máquinas de escribir, se transportaba en la caja en la que estaba incluida. Dicha caja, de dimensiones 34cm×28cm×15cm, pesaba aproximadamente 12kg.

La máquina Enigma fue un dispositivo electromecánico, lo que significa que usaba una combinación de partes mecánicas y eléctricas. El mecanismo estaba basado en una serie de teclas que accionaban los dispositivos eléctricos y provocaban el movimiento de unos cilindros rotatorios. Dichas teclas, compuestas por las letras del alfabeto, eran realmente interruptores eléctricos. Podemos decir que Enigma estaba formada básicamente por tres componentes conectados por cables que, combinados, constituían una compleja máquina para cifrar: un teclado para escribir cada letra del texto en claro; una unidad

[1]Este hecho provocó la confusión de muchos soldados cuando a finales de la guerra se encontraban con uno de estos aparatos.

modificadora formada por tres rotores, un clavijero y un reflector; y un tablero donde quedaba iluminada la letra cifrada.

La supuesta inviolabilidad de la máquina se debe a la que hemos llamado unidad modificadora. En esta unidad se encuentran, como hemos dicho, los tres rotores, un clavijero y un reflector. Los componentes de esta unidad podían ser modificados manualmente cuando se quisiera tanto por el encriptador como por el desencriptador, de modo que, el hecho de que cualquier criptoanalista encontrase la máquina no era de gran importancia, puesto que lo realmente importante sería conocer dichas modificaciones de las que más adelante daremos detalles.

Los componentes de la máquina

Para poder entender el funcionamiento de Enigma, el cual explicaremos más adelante, primero necesitamos ver detalladamente cada una de las partes de las que se compone la máquina.

Gracias a la Figura 2.1 podemos hacernos una idea de la apariencia física de Enigma. Además, nos ofrece la posibilidad observar claramente cada uno de los componentes de la máquina de los que, a continuación, daremos una escrupulosa descripción.

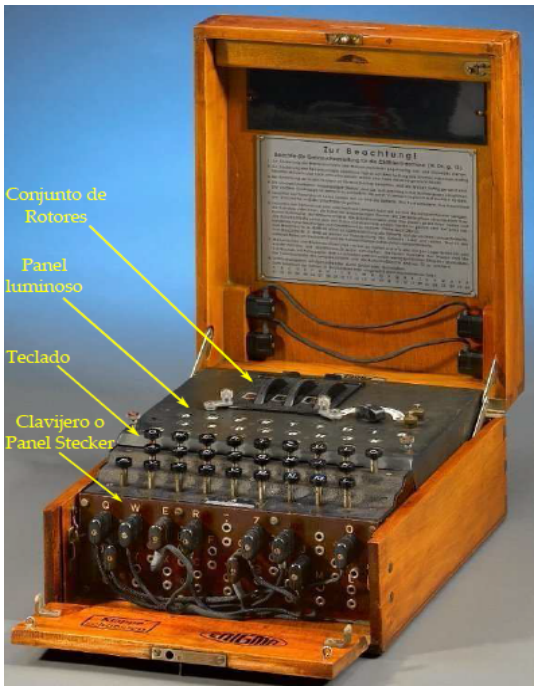


Figura 2.1: Diagrama de las partes de Enigma.

- **Teclado:** Estaba compuesto por 26 teclas, las correspondientes a cada una de las letras del alfabeto. La máquina solamente usaba 26 caracteres ya que la puntuación fue reemplazada por combinaciones de diferentes letras. Algunos ejemplos de dichas combinaciones son: el espacio se sustituye con una `X`, la coma con `ZZ` y el signo de interrogación con `FRAGE` o `FRAQ`[2].

- **Panel luminoso:** Situado justo en frente del teclado. Al igual que este, estaba compuesto por 26 teclas (una por cada letra del alfabeto), aunque ninguna de ellas podía ser pulsada. Debajo de cada una de estas teclas había una bombilla que permitía, al final del procedimiento de cifrado, que la letra codificada se iluminase. La letra iluminada era siempre diferente de la tecla pulsada.

- **Rotores:** Fueron el principal componente de cifrado. Este conjunto estaba formado por tres rotores[3] que no eran sino permutaciones de las letras que actuaban consecutivamente. Cada uno de ellos era un disco de aproximadamente 10cm de diámetro y estaban marcados con los números romanos para distinguirlos: `I, II, III`, ya que aparentemente eran iguales. Todos tenían las letras del alfabeto situadas sobre sus bordes, aunque solo era posible apreciar algunas de ellas. Las que podían verse, situadas en el lugar que sobresale un poco, eran discos dentados que permitían la manipulación de los rotores. Así, en estos rotores era donde el operador llevaba a cabo los ajustes de la máquina. Cada uno de ellos tenía, en una cara, 26 contactos fijos dispuestos de forma concéntrica y, por el otro, los 26 contactos de resorte. Los contactos fijos se conectaban con los de resorte de manera irregular por cables aislados que pasaban a través del corazón del rotor. Cada uno de los rotores se encajaba en la ranura correspondiente de forma que sus contactos de salida se conectaban con los contactos de entrada del rotor siguiente y el tercer y último rotor se conectaba al reflector que, a su vez, unía el contacto de salida del tercer rotor con otro contacto del mismo rotor para realizar el mismo proceso pero en sentido contrario y por una ruta diferente. El impulso eléctrico pasaba de derecha a izquierda a través de los cables de cada rotor. Para hacernos una idea de la apariencia física de éstos podemos observar la Figura 2.2.

[2]Algunos signos de puntuación fueron diferentes en otras partes de las fuerzas armadas. Así, la *Kriegsmarine* (Marina alemana), por ejemplo, sustituía la coma con la `Y` y el signo de interrogación con `UD`.

[3]Dependiendo de la versión, Enigma podría tener más rotores. También era posible añadirlos, lo que supuso un gran alivio para los alemanes, que con el avance de la guerra vieron peligrar la seguridad de Enigma, por lo que incluyeron 2 rotores más. La versión con más rotores y, por lo tanto, la más segura era la utilizada por la *Kriegsmarine*, que llegó a tener hasta 8 rotores. La que nosotros estudiaremos, como hemos dicho, se compone solamente de 3.

Figura 2.2: Rotores de Enigma.

- **Batería:** Se encontraba a la derecha de los rotores y era el componente que hacía funcionar la máquina. La potencia de dicha batería era de 4,5 voltios.

- **Reflector:** Era un elemento establecido en un único eje que podía ser movido con una palanca. No era sino un producto de trasposiciones disjuntas. Esto es, emparejaba las letras dos a dos y cambiaba cada letra por su pareja. El impulso eléctrico era devuelto por el reflector de izquierda a derecha, en sentido contrario al que pasaba a través de los cables de cada rotor. Este elemento conseguía que al codificar un mensaje cifrado, usando las mismas posiciones iniciales de los rotores y los mismos pares de letras interconectadas en el clavijero, se obtuviese el mensaje en claro. Aunque aparentemente el reflector parece muy ventajoso y un elemento clave en la máquina, dio a Enigma la propiedad de que ninguna letra sería cifrada como ella misma. Esto fue un fallo conceptual grave y un error criptográfico que posteriormente sería explotado por los criptoanalistas.

- **Clavijero:** También llamado conmutador o panel *Stecker*[4]. Situado en la parte delantera de la máquina, debajo de las teclas, entre el teclado y el primer rotor. Era un tablero de clavijas, cada una asociada a una letra del alfabeto. Dichas clavijas estaban conectadas mediante cables que podían conmutarse. De esta forma, daban lugar a una permutación que actuaba doblemente, entre el teclado y el banco de rotores y entre este y el panel de lámparas. Así, cada vez que se pulsa una tecla se origina una corriente eléctrica que circula primero por el *Stecker* antes de adentrarse en el banco de rotores. Tras abandonar el banco de rotores, la corriente eléctrica pasa de nuevo por el *Stecker* antes de concluir su viaje en el panel luminoso, produciendo el mismo efecto que antes. Si se conectaban dos de las clavijas, las dos letras conectadas eran intercambiadas en el proceso de cifrado. El sistema de encriptación que estamos estudiando

[4]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 incluido en la versión militar con la intención de aumentar la seguridad, ya que este panel contribuía con más fuerza criptográfica que un rotor adicional.

estaba formado por 6 pares de clavijas[5] o *stecker pairs*, haciendo posible el intercambio de 12 letras.

2.2. El funcionamiento de Enigma

El funcionamiento de la máquina, aparentemente, era bastante sencillo. El operador debía teclear las letras de su mensaje e ir anotando 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. Dicho impulso hacía que la corriente circulara a través del clavijero, luego los rotores derecho, central e izquierdo, se refleja en el reflector y deshace su camino de nuevo a través de los rotores y una vez más a través del clavijero. Al terminar este proceso, la corriente eléctrica concluye su viaje en el panel de lámparas, donde una luz se encendía bajo una de las letras. Aunque más adelante daremos más detalles sobre el circuito eléctrico de Enigma, veamos antes un pequeño esquema:

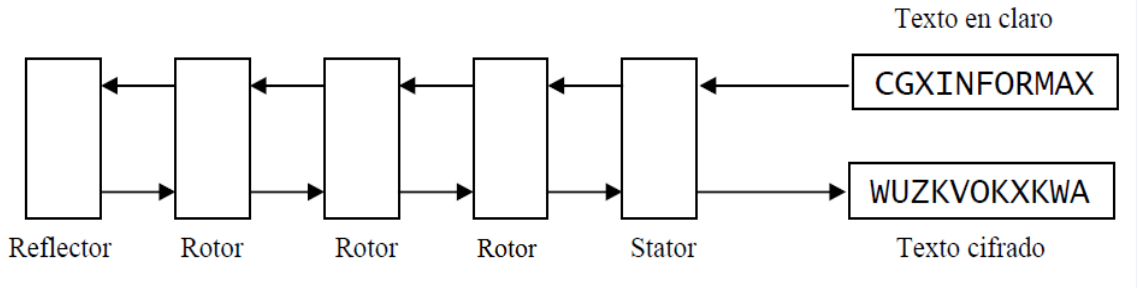


Figura 2.3: Circuito eléctrico de Enigma.

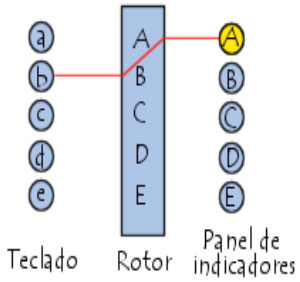
Como hemos dicho anteriormente, los rotores fueron el principal componente de cifrado. Esto se debe a que la complejidad de la máquina reside, en gran parte, en estos elementos. Una de las razones es el hecho de que la pulsación de una tecla provocaba que el primer rotor avanzase una letra en el alfabeto[6]. Podemos imaginar el efecto de un rotor como el de una permutación en las posiciones de las letras del alfabeto, con la característica de que cada vez que se codifica una letra, el rotor se desplaza una posición y, por tanto, la permutación sobre el alfabeto es distinta. Sin embargo, al codificar 26 veces una letra obtendríamos su codificación inicial. Se quiso evitar precisamente esa repetición, nunca deseada en criptografía, razón por la cual la máquina constaba de tres rotores, de manera que al codificar una letra saltaba una posición el rotor más rápido, el que estaba situado más a la derecha. Una vez el rotor

[5]En sucesivas transformaciones de la máquina, con el fin de aumentar su seguridad, el número de pares de clavijas utilizado llegó a ser de hasta 10.

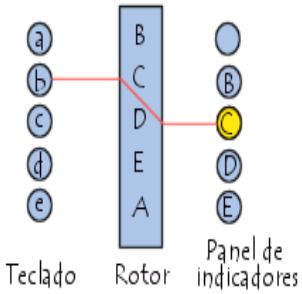
[6]El principio original de esta idea data del siglo IV a.C. Fue un invento del romano Aeneas Tacitus.

derecho diera toda una vuelta, entonces giraba una posición el rotor central hasta llegar al menos rápido que era el de la izquierda. Los rotores central e izquierdo giraban de forma diferente al rotor derecho, ya que además de la rotación ya descrita, rotaban también cuando llegaban hasta la posición de su propia muesca, teniendo en cuenta también que para cada nuevo movimiento del rotor central había que esperar los 26 movimientos del rotor rápido[7].

Veamos con un ejemplo lo que ocurre al presionar una tecla en el tablero. Consideremos que sólo tenemos un rotor. Cuando se presiona, por ejemplo, la letra `B` la corriente pasa a través del rotor y en el panel de luz se enciende la letra `A`. Veámoslo en la siguiente imagen:



Como hemos dicho anteriormente, al presionar una tecla el rotor giraba una tuerca. Por lo tanto, después de presionar, la imagen que ilustraría nuestro ejemplo sería la siguiente:



Una vez observado esto, veamos un ejemplo[8] con el abecedario al completo del camino que seguiría una letra desde su tecleado hasta su cifrado. En dicho ejemplo aparecerán cuatro bloques de dos filas cada uno. La primera fila de cada bloque se corresponde con el abecedario ordenado (puesto para ver el

[7]Estos movimientos podrían complicarse para hacer la máquina aún más segura incluyendo en esta un controlador para el movimiento del segundo y tercer rotor. Esto es, en lugar de que cada rotor girase cuando el anterior hubiera dado una vuelta completa, se podía hacer que el segundo rotor girara, por ejemplo, cuando `N` pasara por la primera posición en el primer rotor (y análogamente, escoger una posición concreta para el giro del tercer rotor).

[8]La situación planteada en el ejemplo ofrece una auténtica configuración de un modelo de Enigma. Extraída de: [10].

ejemplo con mayor claridad), la segunda fila de los tres primeros bloques se corresponde con cada uno de los rotores y la última fila es la correspondiente al reflector.

Primero veremos el caso en el que supondremos que no hay movimiento del primer rotor:

```
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 O V Z N T O W Y H X U S P A I B R C J

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

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

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

Nota: Las letras de color magenta representan el camino de ida a través de los rotores hasta llegar al reflector y las azules representan el camino de vuelta una vez ha actuado éste.

Así, vemos que si pulsamos, por ejemplo `R`, el camino que sigue la letra es:

$$\texttt{R} \longmapsto \texttt{U} \longmapsto \texttt{P} \longmapsto \texttt{E}$$

La letra `E` llegaba finalmente al reflector, donde se produce un nuevo cambio, en este caso, cambia `E` por `Q`, y luego `Q` realiza el camino inverso por los tres rotores:

$$\texttt{E} \longmapsto \texttt{Q} \longmapsto \texttt{Y} \longmapsto \texttt{V} \longmapsto \texttt{I}$$

De esta forma, `R` se cifraba como `I`.

Veamos ahora lo que ocurriría al producirse el movimiento del rotor:

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

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

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

Así, `R` se cifraba como `P`, observando que una misma letra no sería codificada dos veces de la misma forma, por lo que el movimiento del rotor era un elemento que ofrecía más seguridad a la máquina, ya que así se evitaba el posible ataque por análisis de frecuencias.

El diagrama de la Figura 2.4 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.

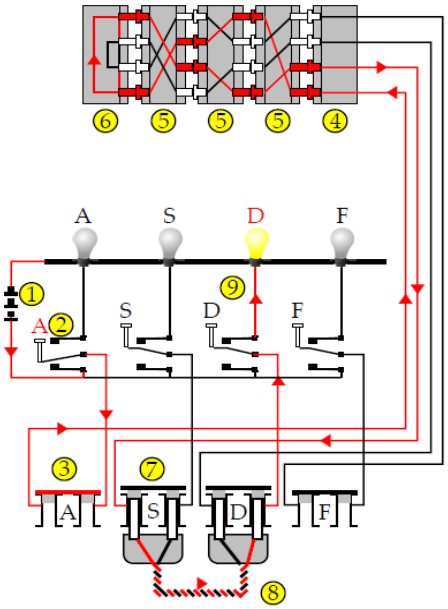


Figura 2.4: Diagrama de funcionamiento de Enigma.

La letra que se iluminaba se encendía dependiendo de los ajustes de la máquina, y esto se podía hacer de muchas formas distintas. Teniendo en cuenta las combinaciones de cada rotor, Enigma tenía un repertorio de $26 \times 26 \times 26 = 17576$ alfabetos de sustitución para cualquier combinación y orden de rotores dada. Así, si el mensaje original no tenía más de 17576 pulsaciones, no habría un uso repetido de un alfabeto de sustitución.

Cabe destacar un hecho que hizo que la máquina fuese aún más difícil de descifrar: los rotores podían ser intercambiados. Es decir, el rotor 1 podría ocupar la posición del rotor 2, el 2 estar en la posición del rotor 3, etc. Esto, junto con el hecho de que al presionar una tecla un rotor girase, provocó que la secuencia de los alfabetos utilizados fuese diferente dependiendo de la posición en la que se encontrase cada rotor, es decir, los rotores colocados de la forma ABC tendrían un alfabeto de sustitución diferente a los colocados de la forma ACB. De esta forma, con tres rotores en tres hendiduras, se obtienen otras $3 \times 2 \times 1 = 6$ combinaciones a considerar (diferentes posiciones que pueden asumir los rotores), por lo que se obtendrían un total de $17576 \times 6 = 105456$ posibles alfabetos.

Debemos tener en cuenta también que el clavijero ocupa una parte muy importante del cifrado de la máquina y que, por lo tanto, hace que nuestra cifra anterior se eleve aún más. Hemos de recordar que el clavijero intercambia 6 pares de letras del panel de enchufes, siendo estos pares iguales, es decir, por ejemplo, `G/R` sería igual a `R/G`, por lo que el número de combinaciones debido a las clavijas sería:

$$\left(\frac{26 \cdot 25}{2}\right) \cdot \left(\frac{24 \cdot 23}{2}\right) \cdot \left(\frac{22 \cdot 21}{2}\right) \cdot \left(\frac{20 \cdot 19}{2}\right) \cdot \left(\frac{18 \cdot 17}{2}\right) \cdot \left(\frac{16 \cdot 15}{2}\right) = 7{,}228208988 \times 10^{13}$$

Además, hay que tener en cuenta la reordenación de las clavijas, esto es, tenemos que dividir la cifra anterior por 6!. Así, el número de combinaciones posibles que ofrece el clavijero asciende a la cantidad de $72282089880000/6! = 100391791500$.

Por lo tanto, las máquinas Enigma podían cifrar un texto utilizando

$$105456 \times 100391791500 \approx 10^{16} \tag{2.1}$$

combinaciones posibles.

2.3. El procedimiento de cifrado

El parámetro de configuración fundamental para operar con Enigma era la clave que tanto emisor como receptor debían conocer. Dicha clave venía

dada en lo que se denominó *Diario de Claves*[9]. Por lo tanto, antes de cifrar el mensaje, el operador encargado de hacerlo debía disponer la máquina según la configuración inicial que se indicaba en la correspondiente *clave del día*. Cada una de ellas constaba de los siguientes datos:

- ***Walzenlage:*** Indicaba el orden en el que se tenían que establecer los rotores en los huecos de la máquina.
- ***Ringstellung:*** Ofrecía la distribución inicial de los anillos de los rotores, que servía para variar la posición de giro de los mismos.
- ***Stecker:*** Indicaba las conexiones del clavijero[10].
- ***Grundstellung:*** Determinaba la posición inicial de los rotores en la máquina, que se configuraba colocando en la ventanilla visible del rotor la letra deseada. Ésto se llevaba a cabo moviendo la ruleta que contenía las letras de la `A` a la `Z`.

Ejemplo.[11] Una *Tageschlüssel* tendría la siguiente apariencia:

Walzenlage	Ringstellung	Stecker	Grundstellung
`I III II`	`X P R`	`AT DS IJ MO WZ XY`	`D E O`

Cuadro 2.1: Ejemplo de *Tageschlüssel*.

La configuración anterior le indicaba al operador que debía poner el primer rotor en el hueco 1 y girarlo hasta la posición `D`, el tercer rotor en el hueco 2 y girarlo hasta `E` y el segundo rotor en el hueco 3 y girarlo hasta la posición `O`. Así mismo debía conectar los cables en el panel *Stecker* con los pares de letras indicados. Una vez configurada la máquina, el operador podía comenzar a cifrar los mensajes.

La operación de la máquina podía realizarla un solo hombre, pero por lo general requería el empleo de dos operadores, uno que leía el mensaje y lo iba pulsando en la Enigma y otro que iba leyendo las letras que se iluminaban y las escribía en un papel. Una vez conocido el mensaje cifrado, este era transmitido a través de la radio en código Morse para ser descodificado por una máquina Enigma receptora ajustada de la misma forma de acuerdo con el

[9]En alemán *Tageschlüssel*. Era un libro de alto mando que recibían los operadores de Enigma con las claves diarias a utilizar en dicho mes. A medida que avanzó la guerra, el número de claves pasó a ser de hasta tres diarias.

[10]Hasta noviembre de 1936 las conexiones del panel *Stecker* fueron exactamente seis. Sin embargo, después de esta fecha y hasta finales de 1938, este número fue variando entre cinco y ocho.

[11]Extraído de: [4].

Diario de Claves. Y aquí es donde juega su papel el reflector. El receptor simplemente tecleará el mensaje cifrado recibido, y el mensaje original aparecería directamente en el panel luminoso.

Operando de este modo parecería imposible descifrar Enigma, ya que el enemigo debería disponer de una máquina como la utilizada por los alemanes junto con el Diario de Claves, algo que resultaba poco probable. Sin embargo, los alemanes se dieron cuenta de que a lo largo de un mismo día generaban un sinfín de mensajes con la misma clave, y esto resultaba un filón para los criptoanalistas, ya que cuantos más mensajes tuvieran más fácil les resultaría descifrar Enigma. Conscientes de ello, llevaron a cabo una serie de órdenes sobre la debida utilización de la máquina[12].

Errores de cifrado

Aunque la imposición de dichas órdenes no tuvo el efecto esperado por los alemanes, veremos a continuación que también se produjeron otros errores que hicieron poner fin a la seguridad de Enigma.

Las normas impuestas fueron 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.
3. Se creó el concepto de *clave del mensaje*[13], también llamada *clave de sesión*. Se hizo con el fin de evitar un intenso tráfico de mensajes cifrados con la misma clave. Consistía básicamente en que cada mensaje enviado debía tener su propia clave. Para que esta clave (elegida al azar por el emisor) fuese conocida por el receptor, el emisor tenía que llevar a cabo una serie de pasos.

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

   Segundo paso: Con dicha configuración tenía que escribir tres letras, por ejemplo `XRS`[14], obteniendo en el panel luminoso `LTV`.

[12]El hecho de señalar una serie de normas estrictas, aunque parezca sensato, hizo que los criptoanalistas se abastecieran de varias pistas que significaron el principio del ataque a Enigma.

[13]En alemán *Spruchschlüssel*.

[14]Este ejemplo se ha llevado a cabo a través de un simulador de la máquina Enigma que se encuentra disponible gratuitamente en la página *www.amenigma.com*. La configuración inicial de la máquina ha sido la propuesta en el cuadro 2.1 que se encuentra en la sección 3 de este mismo capítulo.

Tercer paso: Debía girar los rotores desde su posición inicial (la indicada para ese día por el diario) a la posición de esas tres letras, en este caso `XRS`.

Cuarto paso: Por último, el emisor procedía a codificar el mensaje a enviar.

Cabe destacar que el orden de los rotores y el panel *Stecker* permanecían sin cambios. Una vez enviado el mensaje, el receptor comenzaba leyendo `LTV`, que era la codificación de `XRS` según la clave del día. Así, el receptor, teniendo la máquina configurada de igual modo que el emisor, tecleaba esas tres primeras letras (en nuestro caso `LTV`) y veía en el panel de luces `XRS`. Entonces procedía a girar los rotores a esa disposición, `XRS`, y tecleaba el resto del mensaje, obteniendo el original.

De este modo, cada mensaje se cifraba con una posición diferente de los rotores. Como hemos dicho anteriormente, la clave era elegida al azar por el emisor. 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. Así que, con el fin de evitar estos errores, los alemanes establecieron la norma de que la clave del mensaje debía ser cifrada dos veces seguidas, estando el mensaje, de esta forma, encabezado por seis letras. Entonces, el emisor tecleaba `XRSXRS`, obteniendo en el panel luminoso `LTVQJX`, al contrario de lo que haría el receptor, que recibiría `LTVQJX` y vería en el panel luminoso `XRSXRS`. 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 descifrado. Así, los alemanes creyeron que la máquina sería inviolable. Sin embargo, esta norma ofreció a los criptoanalistas un punto de partida para comenzar a descifrar Enigma, ya que de esta forma, se podía observar que la primera letra coincidía con la cuarta, la segunda con la quinta y la tercera con la sexta.

Esto último se explica de la siguiente forma: si tenemos un número suficiente de mensajes (80 aproximadamente) dados en un mismo día, entonces, en general, todas las letras del alfabeto aparecerán en los seis lugares al principio de los mensajes. En cada lugar estas formarán una transformación única de la disposición de las letras en ellas mismas, es decir, serán permutaciones. Estas permutaciones no eran conocidas por el criptoanalista, pero sí lo eran las permutaciones compuestas por las transformadas de las primeras letras a las cuartas, las segundas a las quintas y las terceras a las sextas.

El fin de Enigma se produjo, entre otras cosas, por el incumplimiento de algunos de los principios de Auguste Kerckhoffs[15]. Estos principios fueron enun-

[15]Lingüista y criptógrafo holandés cuyos trabajos significaron una auténtica renovación para las técnicas criptográficas del momento.

ciados en 1883 en uno de sus ensayos sobre criptografía militar en la Revista de Ciencias Militares francesa y debían cumplirse para poder diseñar cualquier sistema criptográfico eficiente. Los seis principios fundamentales eran:

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

Como podemos observar, los alemanes incumplieron casi todos estos principios. Primero, hemos visto que con el avance de la guerra fueron haciendo cambios a la máquina con el fin de hacerla más segura, con lo que confiaron la efectividad de ésta en el hecho de mantenerla en secreto, incumpliendo así el punto 2. Segundo, hemos podido comprobar que la clave a utilizar era elegida al azar por el emisor, sin embargo, para empezar a hacer funcionar la máquina debían recurrir a notas escritas, incumpliendo así el punto 3. Tercero, Enigma se componía de un teclado con 26 caracteres correspondientes a las letras del alfabeto, por lo que los criptogramas no podrían dar resultados numéricos, incumpliendo así el punto 4. Cuarto, como hemos explicado anteriormente, la máquina podía ser operada por un sólo hombre, aunque normalmente lo hicieran entre varios, por lo que no podemos afirmar que se incumpliese el punto 5. Y, por último, podemos decir que el sistema resultaba fácilmente utilizable, con lo que tampoco incumplía el punto 6. Podemos concluir que incumplieron 3 de los 6 principios fundamentales.

A los errores anteriores hay que añadir algunos más.

- **Antigüedad de Enigma:** Al comenzar la guerra la máquina ya tenía diez años de vida, más que suficientes para haberla podido estudiar con tranquilidad y sólo a finales de la guerra fueron incluidos dos nuevos rotores.
- **Gran error humano:** Los encriptadores, por aburrimiento o por fuerza de la costumbre, empezaron a elegir como clave constantemente los mismos grupos de letras, como por ejemplo `QAZ` o `WSX`, en lugar de usar combinaciones siempre diferentes.

- **Rígida disciplina alemana:** Se empezaron a generar mensajes con formatos de texto constantemente repetidos y que identificaban fácilmente la procedencia de los mismos. Un ejemplo de ello es la emisión todos los días a las 00:00 horas reportando indicativos de estaciones, frecuencias, horarios de transmisión, etc.

Los errores antes mencionados fueron debidos a la confianza, en exceso, que los alemanes depositaron en la máquina. Cierto es que Enigma fue muy segura, por lo que parece lógico confiar en ella. Sin embargo, jamás debieron bajar la guardia, ya que eso supuso el principio del fin de Enigma.

Capítulo 3

Resultados matemáticos necesarios para el ataque

El trabajo de los polacos se basó fundamentalmente en el estudio de la repetición de patrones. Teniendo en cuenta lo expuesto al final del capítulo anterior, podemos observar que el patrón más obvio de la encriptación de Enigma era la repetición de la clave del mensaje. Este hecho les proporcionó una vía para comenzar el ataque.

3.1. Primer intento de búsqueda de la desencriptación del código Enigma

Los polacos realizaron un gran avance en el estudio del funcionamiento de Enigma mediante el análisis de los patrones de repetición. Con este método llegaron a descubrir que las cadenas de caracteres cifrados estaban directamente relacionados con la posición de los rotores de la máquina[1]. Sin embargo, se encontraron con nuevas dificultades: el desconocimiento de la distribución del cableado interno de la máquina y las sucesivas modificaciones de dicho cableado, producidas por los alemanes con el fin de conservar la integridad de sus comunicaciones.

El punto de partida para este primer intento de ataque fue la intercepción de algunos mensajes por parte de las estaciones polacas de radiomonitoreo. Estos mensajes fueron usados para la reconstrucción de las claves de Enigma. Así, el objetivo era completar lo que se denominó *tabla de relaciones* que no buscaba otra cosa que relacionar todas las letras del alfabeto. Como la clave del mensaje se tecleaba dos veces, se deducía que la 1^a y la 4^a letra de la codificación correspondían a la misma letra del mensaje original. Al igual que con la 2^a y la 5^a y con la 3^a y la 6^a. De esta forma, si durante un día

[1]Este descubrimiento lo llevó a cabo Marian Rejewski, matemático del que dimos detalles en el primer capítulo y cuyas hazañas fueron claves para el posterior ataque a Enigma.

se conseguían suficientes mensajes, todas las letras del alfabeto aparecerían al principio de dichos mensajes. Veamos cómo se construía dicha tabla[2]. El primer paso a seguir era observar las seis primeras letras de cada mensaje interceptado y estudiar su relación. Si por ejemplo veíamos `QWERTY`, que se corresponde con la codificación de la clave del mensaje usando la clave del día, podíamos observar que `Q` y `R` eran codificaciones de la misma letra. De esta forma, si tenemos, por ejemplo[3], los siguientes 4 mensajes:

Mensaje 1: `L O K R G M`
Mensaje 2: `M V T X Z E`
Mensaje 3: `J K T M P E`
Mensaje 4: `D V Y P Z X`

vemos que en el primer mensaje `L` y `R` están relacionadas, así como `M` y `X`, `J` y `M`, y `D` y `P` en los otros tres mensajes. Por lo tanto, obtendríamos las siguientes relaciones:

```
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
      P           M   R X
```

El siguiente paso a seguir para la construcción de la tabla es interceptar el mayor número de mensajes posible y, así, poder completar la segunda línea del ejemplo anterior, correspondiente a las relaciones de cada letra del alfabeto con su codificada. De este modo, después de interceptar un gran número de mensajes, la tabla de relaciones para un día determinado se completaría del siguiente modo:

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

Cuadro 3.1: Ejemplo de *tabla de relaciones*.

Una vez construida la tabla, el objetivo era encontrar algún patrón que se pudiera deducir de ella. Estaba claro que dicha tabla era el reflejo de la disposición inicial de Enigma con la clave del día, por lo que era de vital importancia centrarse en estudiar esas relaciones para, así, poder obtener alguna estructura que le indicara la clave del día, el anhelado objetivo. Después de intentar encauzar el estudio desde diferentes puntos de vista, Rejewski se centró en lo que posteriormente se llamaría *cadenas de letras*. Estas cadenas se construyen

[2]Para poder entender mejor el procedimiento, solo tendremos en cuenta la relación de la 1ª letra con la 4ª. Para las demás el proceso es análogo.

[3]Extraído de *http://portierramaryaire.com/arts/enigma_1.php*.

de la siguiente forma: teniendo en cuenta el Cuadro 3.1, se trata de formar una cadena cerrada empezando con una letra de la fila superior, buscando su relación en la fila inferior y, a su vez, volviendo a buscar esta última letra en la fila superior y su relación con la fila inferior, y así hasta llegar a la letra con la que comenzamos. Veamos, en nuestro caso, como quedaría formada dicha cadena. Vemos en el Cuadro 3.1 que la `A` de la fila superior está relacionada con la `F` de la inferior; la `F` de la superior está relacionada con la `W` de la inferior; la `W` de la superior está relacionada con la `A` de la inferior, que es la letra con la que comenzamos la cadena, quedando, así, cerrada. Por último, Rejewski desarrolló todas las cadenas de la tabla[4], apuntando en cada una de ellas el número de conexiones que tenían, obteniendo lo siguiente:

```
          A - F - W - A                 3 conexiones
B - Q - Z - K - V - E - L - R - I - B    9 conexiones
    C - H - G - O - Y - D - P - C        7 conexiones
    J - M - X - S - T - N - U - J        7 conexiones
```

Una vez construidas las cadenas, Rejewski observó que estas cambiaban cuando lo hacía la clave del día, llegando a la conclusión de que estas cadenas eran el reflejo de la disposición de los rotores y que el clavijero no influía en ellas ni en sus longitudes. De esta forma, observando (2.1) vemos que ahora solo deberíamos preocuparnos de las 105456 claves debidas a la disposición de los rotores y no de los billones de claves posibles de las que nos teníamos que ocupar antes. Tediosa tarea, pero ya susceptible de ser realizada manualmente.

Gracias a esos estudios y a numerosas observaciones, Rejewski pronto se dio cuenta de que podía resolver su problema con *teoría de grupos* y permutaciones.

3.2. El método de las permutaciones. Fundamentación teórica

Como avanzábamos con el título de este capítulo, para poder llevar a cabo el ataque se necesitaron varios resultados matemáticos, los cuales expondremos a continuación.

Sea $\Gamma_n = \{x_1, x_2, ..., x_n\}$ un conjunto finito de n elementos, el ejemplo de grupo finito más usado en la *teoría de grupos* es el grupo de las permutaciones de Γ_n.

[4]Estas cadenas se forman sin repetir letras, es decir, comenzamos con la letra `A` y formamos su cadena, si la `B` aparece en la cadena de `A`, se omite, si no formamos su cadena correspondiente, y así sucesivamente.

Permutaciones

Intuitivamente, decimos que una permutación es la variación del orden o de la disposición de los elementos de un conjunto. Es decir, podemos considerar que una permutación es una reordenación de elementos.

Definición 3.2.1 *Si X es un conjunto no vacío, una* ***permutación*** *de X es una función biyectiva $\alpha : X \to X$.*

Definición 3.2.2 *Si X es un conjunto no vacío, el* ***grupo simétrico*** *de X, denotado por S_X, es el grupo cuyos elementos son las permutaciones de X y cuya operación binaria es la composición de funciones.*

Como adelantábamos anteriormente, es de particular interés el caso especial en el que X es finito. En dicho caso, siendo $X = \{x_1, x_2, ..., x_n\}$, nosotros escribiremos S_n en lugar de S_X, y llamaremos S_n al grupo simétrico de grado n, o al grupo simétrico de n letras, teniendo en cuenta que $|S_n| = n!$, donde $|Y|$ denota el número de elementos de un conjunto Y.

Sea X el conjunto $\{1, 2, ..., n\}$. Una forma de denotar una permutación α de X es mediante su representación en una matriz de correspondencias de la forma:

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \end{pmatrix}$$

lo cual significa que $\alpha(k) = \alpha_k$. Por lo tanto, si denotamos:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

esto quiere decir que $\alpha(1) = 3$, $\alpha(2) = 2$ y $\alpha(3) = 1$.

Si, además, definimos otra matriz de la siguiente forma:

$$\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

tenemos que α y β son permutaciones de $\{1, 2, 3\}$.

Además, la composición de permutaciones es, claramente, una permutación y cumple las siguientes propiedades:

- Asociativa: $\alpha \circ (\beta \circ \tau) = (\alpha \circ \beta) \circ \tau \quad \forall \alpha, \beta, \tau$.

- Existe una permutación I tal que: $\alpha \circ I = \alpha = I \circ \alpha \quad \forall \alpha$. Dicha permutación I es la aplicación identidad, por lo tanto cumple: $I(x) = x \quad \forall x \in X$.
- Existe una permutación α^{-1} tal que $\alpha \circ \alpha^{-1} = I = \alpha^{-1} \circ \alpha \quad \forall \alpha$. Dicha permutación α^{-1} es la aplicación inversa de α.

Así, el conjunto S_n de las permutaciones de X con la composición es, pues, un grupo.

El producto de dos permutaciones se interpreta como composición de aplicaciones, por lo que escribiremos, a veces, $\alpha\beta$ en lugar de $\alpha \circ \beta$. De esta forma, el producto de dos permutaciones cumpliría lo siguiente: $\alpha\beta(k) = \alpha(\beta(k)),\ \forall k \in \{1, 2, ..., n\}$. Aunque algunos autores realizan el producto en el orden contrario, es decir, aplicando primero β y después α. Los productos de estas permutaciones son[5]:

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\beta\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Así, podemos observar que $\alpha\beta \neq \beta\alpha$. De ello se deduce que S_3 no es conmutativo y, por lo tanto, no es abeliano. De esta forma, podemos enunciar la siguiente proposición.

Proposición 3.2.1 *Si $n \geq 3$, S_n no es es conmutativo.*

Demostración. Se sigue del ejemplo anterior. ◇

Definición 3.2.3 *Un elemento k se denomina **fijo** por una permutación α si $\alpha(k) = k$.*

Definición 3.2.4 *Se denomina **soporte** de la permutación al conjunto de elementos $\{1, 2, ..., n\}$ que no son fijos por una permutación α, y se denota A_α.*

Definición 3.2.5 *Sean α y β dos permutaciones, se dice que estas son **disjuntas** si $A_\alpha \cap A_\beta = \emptyset$.*

[5]Hemos realizado estos productos de acuerdo a la definición anterior. Así, en el primer caso, por ejemplo, el producto se realizaría del siguiente modo: $\alpha\beta(1) = \alpha(\beta(1)) = \alpha(2) = 2$; $\alpha\beta(2) = \alpha(\beta(2)) = \alpha(3) = 1$; $\alpha\beta(3) = \alpha(\beta(3)) = \alpha(1) = 3$.

En el caso de nuestras permutaciones anteriormente definidas, α y β, podemos observar:

- Elementos fijos: en α sólo aparece un elemento fijo: 2, y en β no aparece ninguno.
- Soporte: $A_\alpha = \{1, 3\}$ y $A_\beta = \{1, 2, 3\}$.

Entonces, $A_\alpha \cap A_\beta = \{1, 3\} \cap \{1, 2, 3\} = \{1, 3\} \neq \emptyset$. Por lo tanto, α y β no son disjuntas.

Veamos ahora un ejemplo en el que se cumpla que dos permutaciones sean disjuntas.

Sean σ y τ las siguientes permutaciones:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 5 \end{pmatrix}; \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 4 & 1 \end{pmatrix}$$

Entonces, en este caso tenemos:

- Elementos fijos: en σ aparecen dos elementos fijos: $\{1, 5\}$, y en τ aparecen tres: $\{2, 3, 4\}$.
- Soporte: $A_\sigma = \{2, 3, 4\}$ y $A_\tau = \{1, 5\}$.

Entonces, $A_\sigma \cap A_\tau = \{2, 3, 4\} \cap \{1, 5\} = \emptyset$. Por lo tanto, σ y τ son disjuntas.

Como hemos visto el producto de permutaciones no es conmutativo, en general. Sin embargo, el concepto de disyunción de permutaciones nos permite enunciar resultados como el siguiente.

Teorema 3.2.1 *Dos permutaciones disjuntas conmutan entre sí. Es decir, si α y β son dos permutaciones disjuntas, entonces $\alpha\beta = \beta\alpha$.*

Demostración. Sea $k \in \{1, 2, ..., n\}$, consideramos los siguientes casos:

1. k es un elemento fijo en α y β.
   En este caso se tiene:

$$\left.\begin{array}{ll} \alpha\beta(k) = \alpha(k) & = k \\ \beta\alpha(k) = \beta(k) & = k \end{array}\right\} \implies \alpha\beta(k) = \beta\alpha(k)$$

   Entonces, α y β conmutan para k.

2. k es un elemento fijo en β y no en α.
   Como k es un elemento fijo en β, tenemos que $\beta(k) = k$. Supongamos que $\alpha(k) = l$, con $l \neq k$. Como l no es fijo en α, y α y β son disjuntas, entonces l será fijo en β. Por lo tanto, tenemos que $\beta(l) = l$. Entonces, tenemos:

$$\left.\begin{array}{ll} \alpha\beta(k) = \alpha(k) & = l \\ \beta\alpha(k) = \beta(l) & = l \end{array}\right\} \implies \alpha\beta(k) = \beta\alpha(k)$$

   Por lo tanto, α y β conmutan para k.

3. k es un elemento fijo en α y no en β. Análogo al anterior.

Entonces, queda demostrado que $\alpha\beta = \beta\alpha$. ◇

Uno de los problemas fundamentales cuando se estudian estructuras algebraicas es poder factorizar los elementos de la estructura en términos de elementos más simples. En el caso de las permutaciones se pudo solventar este problema con el concepto de *ciclo*.

Ciclos

Un *ciclo* es un tipo especial de permutación que fija cierto número de elementos (quizás ninguno) mientras que mueve cíclicamente el resto.

Definición 3.2.6 *Una permutación $\alpha \in S_n$ se denomina **ciclo**, si existe $I = \{a_1, a_2, ..., a_m\} \in \{1, 2, ..., n\}$ tal que:*

- *Se tienen las relaciones $\alpha(a_k) = \alpha(a_{k+1}), \forall i = 1, 2, ..., m-1$, y $\alpha(a_m) = a_1$.*
- *Todos los elementos de $\{1, 2, ..., n\}$ distintos de los a_k son fijos para la permutación α. Es decir, $\alpha(j) = j, \forall j \notin I$.*

Definición 3.2.7 *Sea $m \in \mathbb{N}$ el número usado en la definición anterior. Se denomina **longitud** del ciclo a dicho número m.*

Definición 3.2.8 *Sea $\alpha \in S_n$ una permutación. Se define el **orden** de α como* $\text{mín}\{k \geq 1 : \alpha^k = id\}$.

Nota: En el caso de los ciclos los conceptos de *longitud* y *orden* coinciden.

Notación: Sea α un ciclo y m su orden. Dicho orden lo denotaremos como $o(\alpha) = m$. De esta forma, diremos que α es un $m - ciclo$.

Ejemplo.

- En S_5 un ciclo de longitud 5 es $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 1 & 4 \end{pmatrix}$
- En S_5 un ciclo de longitud 2 es $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$

Notación: Para representar permutaciones de acuerdo con las definiciones anteriores usaremos una notación cíclica. Así, denotaremos al ciclo α de longitud m por $(a_1\ a_2\ ...\ a_m)$.

Con esa notación se tiene: $(a_1\ \ a_2\ \ ...\ \ a_m) = (a_2\ \ ...\ \ a_m\ \ a_1) = \cdots = (a_m\ a_1\ ...\ a_{m-1})$.

Ejemplo.

- La permutación $\alpha \in S_8$ dada por $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 5 & 2 & 7 & 4 & 8 & 6 \end{pmatrix}$ es un ciclo, se denota por $\alpha = (1\ 3\ 5\ 7\ 8\ 6\ 4\ 2)$ y su longitud es 8.
- La permutación $\beta \in S_7$ dada por $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 1 & 3 & 4 & 7 & 6 & 2 \end{pmatrix}$ es un ciclo, se denota por $\beta = (1\ 5\ 7\ 2)$ y su longitud es 4.

Como adelantamos, el concepto de *ciclo* se utiliza, entre otras cosas, para factorizar las permutaciones. Constancia de ello se tiene gracias a un teorema que enunciaremos a continuación.

Teorema 3.2.2 *Toda permutación $\alpha \in S_n$, con $\alpha \neq I$, se puede expresar de manera única, salvo orden de los factores, como producto de ciclos disjuntos de longitud ≥ 2.*

Demostración. La prueba consiste en dos etapas.

Existencia: Sea

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \end{pmatrix}$$

una permutación arbitraria de S_n. Se nos presentan dos casos:

1. $\alpha = 1$.

2. $\alpha \neq 1$. Sea k un número tal que $\alpha(k) \neq k$, construimos entonces $\alpha^2(k)$, $\alpha^3(k)$, $\alpha^4(k)$, ... hasta que, siguiendo este procedimiento, volvamos a obtener k. Al número de pasos que debamos realizar hasta volver a obtener k lo denotaremos $i+1$. De esta forma, hemos construido el ciclo $(k\ \alpha(k)\ \alpha^2(k)\ \cdots\ \alpha^i(k))$, el cual describe parte de la permutación α. De nuevo tenemos dos casos:

   a) El resto de la permutación no contiene números o los números que contiene son fijos.

   b) El resto de la permutación contiene números que no son fijos. En este caso, tendríamos que repetir el procedimiento anterior con ese resto y, así, sucesivamente. Tras realizar un número finito de pasos se obtendría la descomposición.

Unicidad: Supongamos que

$$\begin{cases} \alpha = a_r \cdots a_2 \cdot a_1 \\ \alpha = b_s \cdots b_2 \cdot b_1 \end{cases}$$

son dos descomposiciones de α en producto de ciclos disjuntos. Sea k_1 un número que es movido por α. Entonces, es evidente que k_1 debe estar en un ciclo y sólo uno de $\{a_r, ..., a_2, a_1\}$, y de igual forma, en sólo uno de $\{b_s, ..., b_2, b_1\}$. Como estos ciclos son disjuntos, entonces conmutan. Por tanto, podemos suponer que k_1 está en a_1 y en b_1. Por otra parte, sabemos que los números que aparecen en a_1 (respectivamente b_1) son fijos por el resto de los ciclos a_i (respectivamente b_i), entonces el elemento k_1 ha de transformarse en un mismo elemento k_2 mediante a_1 (respectivamente b_1). Por la misma razón, k_2 debe transformarse en un mismo elemento k_3 mediante a_1 y b_1, y así sucesivamente. Por lo tanto, $a_i = b_i$. De esta forma, repitiendo el procedimiento, se deduce que $r = s$ y que los ciclos a_i y b_i son iguales. ◇

Ejemplo. Sea α la permutación dada en S_8

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 7 & 6 & 3 & 4 & 1 & 8 \end{pmatrix}$$

su descomposición en ciclos disjuntos sería $\alpha = (1\ 5\ 3\ 7)\ (2)\ (4\ 6)\ (8)$. Sin embargo, los ciclos de longitud 1 suelen omitirse, sobreentendiéndose que los números que no aparecen corresponden a ciclos de longitud 1. Teniendo en cuenta esto, escribiríamos $\alpha = (1\ 5\ 3\ 7)\ (4\ 6)$.

Hemos visto que la forma de descomponer una permutación como producto de ciclos disjuntos es única. Esta descomposición no es única sin la restricción de la disyunción. Sin embargo, una puede transformarse en la otra.

Ejemplo. Sean $\alpha = (1\ 2)$ y $\beta = (1\ 3\ 4\ 2\ 5)$ dos ciclos. Supongamos que $\tau = \alpha\beta$. Esta multiplicación es simplemente la composición. Por lo que el producto se haría del siguiente modo:

$$\left.\begin{array}{ll} \tau(1) = \alpha(\beta(1)) & = \alpha(3) = 3 \\ \tau(3) = \alpha(\beta(3)) & = \alpha(4) = 4 \\ \tau(4) = \alpha(\beta(4)) & = \alpha(2) = 1 \end{array}\right\} \Longrightarrow (1\ 3\ 4)$$

$$\left.\begin{array}{ll} \tau(2) = \alpha(\beta(2)) & = \alpha(5) = 5 \\ \tau(5) = \alpha(\beta(5)) & = \alpha(1) = 2 \end{array}\right\} \Longrightarrow (2\ 5)$$

Por lo tanto, tenemos $(1\ 2)(1\ 3\ 4\ 2\ 5) = (1\ 3\ 4)(2\ 5)$.

Así, vemos que la descomposición en ciclos puede ser transformada en un producto de ciclos disjuntos.

Nota:

- Sea $\alpha = (a_1\ a_2 \cdots a_n)$ un ciclo de longitud m. Entonces $\alpha^{-1} = (a_m \cdots a_2\ a_1)$ también es un ciclo de longitud m.
- Sea $\alpha = \alpha_1\alpha_2 \cdots \alpha_l$ un producto de ciclos disjuntos. Entonces $\alpha^{-1} = \alpha_1^{-1}\alpha_2^{-1} \cdots \alpha_l^{-1}$.

Lema 3.2.1 *Si $k, l \geq 0$, entonces:*

$$\begin{cases} (a\ b)(a\ c_1 \cdots c_k\ b\ d_1 \cdots d_l) = (a\ c_1 \cdots c_k)(b\ d_1 \cdots d_l) \\ (a\ b)(a\ c_1 \cdots c_k)(b\ d_1 \cdots d_l) = (a\ c_1 \cdots c_k\ b\ d_1 \cdots d_l) \end{cases}$$

Demostración. El lado izquierdo envía:

$$\begin{array}{llll} a \mapsto c_1 \mapsto c_1, & c_i \mapsto c_{i+1} \mapsto c_{i+1}\,(i < k), & c_k \mapsto b \mapsto a \\ b \mapsto d_1 \mapsto d_1, & d_j \mapsto d_{j+1} \mapsto d_{j+1}\,(j < l), & d_l \mapsto a \mapsto b \end{array}$$

Procediendo del mismo modo en la parte derecha, llegamos a que ambas permutaciones son iguales.
Para la segunda ecuación, simplemente tenemos que multiplicar la parte izquierda de ambos lados de la primera ecuación por $(a\ b)$. ◇

Proposición 3.2.2 *Sea $\alpha \in S_n$. Sea $\alpha = \alpha_1 \cdot \alpha_2 \cdots \alpha_m$ la descomposición de α en producto de ciclos disjuntos. Entonces $o(\alpha) = lcm(o(\alpha_1), o(\alpha_2), ..., o(\alpha_m))$.*

Demostración. Elemental. ◇

Ejemplo. Calculemos el orden de la permutación α del ejemplo anterior. Recordemos que la descomposición de α en ciclos disjuntos era la siguiente $\alpha = (1\ 5\ 3\ 7)\ (4\ 6)$. Por lo tanto, de acuerdo a la proposición anterior, tendríamos que el orden de α será igual a $\text{lcm}(o(\alpha_1), o(\alpha_2)) = \text{lcm}(4, 2) = 4$.

Transposiciones

Definición 3.2.9 *Se denomina* ***transposición*** *a un ciclo de longitud 2 o 2-ciclo, el cual intercambia meramente un par de elementos.*

Teorema 3.2.3 *Toda permutación $\alpha \in S_n$ puede representarse, no necesariamente de manera única, como producto de transposiciones.*

Demostración. Dado que hemos probado que toda permutación se puede descomponer como producto de ciclos disjuntos, es suficiente probar que todo ciclo se puede descomponer como producto de transposiciones. Sea pues, $\alpha = (a_1\ a_2\ \cdots\ a_m)$ es claro que

$$\alpha = (a_1\ a_2\ \cdots\ a_m) = (a_1\ a_m)\ \cdots\ (a_1\ a_3)\ (a_1\ a_2)$$

◇

De acuerdo con lo anterior, es necesario enfatizar dos resultados sobre el producto de transposiciones:

- No es conmutativo, en general. Así, por ejemplo,

$$(1\ 2\ 3) = (1\ 3)(1\ 2) \neq (1\ 2)(1\ 3)$$

- Los factores que componen el producto no se determinan de forma única. Así, por ejemplo,

$$(1\ 2\ 3) = (1\ 3)(1\ 2) = (2\ 3)(1\ 3) = (1\ 3)(4\ 2)(1\ 2)(1\ 4)(2\ 3)(2\ 3)$$

Tras observar los anteriores resultados nos surge la duda de si existe alguna singularidad en dicho producto. Demostraremos, entonces, que sí la hay, esta es: el número de factores no puede ser par e impar a la vez.

Definición 3.2.10 *Una permutación $\alpha \in S_n$ se denomina permutación* ***par*** *si se puede descomponer como un número par de transposiciones. En caso contrario, diremos que es* ***impar****.*

Proposición 3.2.3 *La permutación identidad no se puede expresar como producto de un número impar de transposiciones.*

Demostración. Basaremos nuestra demostración en el siguiente hecho: si en la expresión del producto:

$$P = \prod_{i,j}(j - i)$$

donde $1 \leq i < j \leq n$, $i, j \in \{1, 2, ..., n\}$ permutamos las i, j según una transposición, obtenemos la misma expresión con signo contrario.
Sea $\alpha \in S_n$ una permutación, escribimos:

$$\alpha \cdot P = \prod_{i,j}(\alpha(j) - \alpha(i))$$

Veamos cuáles son los factores de $\alpha \cdot P$, en caso de que $\alpha = (h, k)$, $h < k$.

- Si i, j son diferentes de h, k, entonces $\alpha(j) - \alpha(i) = j - i$. Se ha producido solamente un cambio de posición.
- Si $i < h < k$, el factor $h - i$ de P pasa a ser $k - i$ en $\alpha \cdot P$ y el factor $k - i$ de P pasa a ser $j - h$ en $\alpha \cdot P$. Nuevamente, se ha producido solo un cambio de posición.
- Si $h < i < k$, el factor $i - h$ de P pasa a ser $i - k$ en $\alpha \cdot P$, el factor $k - i$ de P pasa a ser $h - i$ en $\alpha \cdot P$. Se han producido cambios de posición y signo. Sin embargo, como el cambio de signo se ha producido dos veces, no afecta al producto.
- Si $i = h < k = j$, el factor $k - h$ de P pasa a ser $h - k$ en $\alpha \cdot P$. Este es el único cambio de signo que afecta al producto.

Obtenemos entonces:

$$\alpha \cdot P = -P$$

Supongamos ahora que:

$$I = \tau_n \cdots \tau_2 \cdot \tau_1$$

donde las τ_i son transposiciones.
Apliquemos sucesivamente las transposiciones $\tau_1, \tau_2, ..., \tau_n$ a P. Así, obtenemos $(-1)^n \cdot P$.
Por otro lado, aplicar $\tau_1, \tau_2, ..., \tau_n$ equivale a aplicar la identidad y, por tanto, el resultado ha de ser P. Es decir, $(-1)^n \cdot P = P$, de donde se deduce que n es par. ◇

Teorema 3.2.4 *Sea $\alpha \in S_n$ una permutación. Si $\alpha = a_1 \cdots a_r = b_1 \cdots b_s$ son dos descomposiciones de α como producto de transposiciones, entonces r y s tienen la misma paridad. Es decir, α no puede ser simultáneamente par e impar.*

Demostración. Multiplicando los dos productos por b_1 a la izquierda y teniendo en cuenta que $b_1 \cdot b_1 = I$, obtenemos:

$$b_1 \cdot a_1 \cdots a_r = b_2 \cdots b_s$$

Ahora, multiplicamos a la izquierda por b_2, después por b_3 y así sucesivamente, hasta llegar a b_s. De esta forma, obtenemos:

$$b_s \cdots b_1 \cdot a_1 \cdots a_r = I$$

Entonces, usando la proposición anterior, obtenemos que $r + s$ es par y, por tanto, r y s son ambos pares o ambos impares. ◇

Definición 3.2.11 *Sean α, $\beta \in S_n$ dos permutaciones. Se dice que son **conjugadas** si existe otra permutación $\tau \in S_n$ tal que $\beta = \tau\alpha\tau^{-1}$.*

Definición 3.2.12 *Se dice que los elementos α, $\beta \in S_n$ tienen la **misma estructura en ciclos**, si para cada $r \geq 1$ el número de r-ciclos en α es igual al número de r-ciclos en β.*

Teorema 3.2.5 *Sean α, $\beta \in S_n$, entonces α y β son conjugadas $\iff$ tienen la misma estructura en ciclos.*

Demostración. Sea $\alpha = (a_1 \cdots a_k)$ un k - ciclo en S_n y $\tau \in S_n$, pongamos $\tau(a_i) = b_i$, entonces

$$\tau\alpha\tau^{-1}(b_i) = \tau\alpha(a_i) = \tau(a_{i+1}) = b_{i+1} \qquad \forall i \leq r-1$$

Definiendo $b_{k+1} = b_l$ se tiene $\tau\alpha\tau^{-1} = (\tau(a_1) \cdots \tau(a_k))$; supongamos que $\alpha = \alpha_1 \cdots \alpha_m$ es la descomposición de α como producto de ciclos disjuntos (incluyendo ciclos de longitud uno), entonces para cualquier $\tau \in S_n$,

$$\tau\alpha\tau^{-1} = \tau\alpha_1\tau^{-1}\tau\alpha_2\tau^{-1} \cdots \tau\alpha\tau^{-1}$$

de esto se tiene, por lo anterior, que α y cualesquiera de sus conjugados tienen la misma estructura en ciclos.
Supongamos que α y β tienen la misma estructura en ciclos, digamos

$$\alpha = (a_1\ a_2\ \cdots)(b_1\ b_2\ \cdots)\cdots$$

$$\beta = (c_1\ c_2\ \cdots)(d_1\ d_2\ \cdots)\cdots$$

en donde los ciclos aparecen en orden creciente en cada una de las permutaciones. Definiendo $\tau(a_i) = c_i$, $\tau(b_i) = d_i$, y así sucesivamente, uno verifica que $\tau\alpha\tau^{-1} = \beta$. ◇

Teorema 3.2.6 *Si dos permutaciones que tienen la misma estructura en ciclos se descomponen únicamente como producto de transposiciones disjuntas, entonces su producto consistirá en pares de ciclos disjuntos de la misma longitud.*

Demostración. Rejewski realizó la demostración de este teorema y argumentó su prueba del siguiente modo. Si tenemos las siguientes permutaciones:

$$\left.\begin{array}{l} X = (a_1\ a_2)(a_3\ a_4)(a_5\ a_6)\cdots(a_{2k-3}\ a_{2k-2})(a_{2k-1}\ a_{2k}) \\ Y = (a_2\ a_3)(a_4\ a_5)(a_6\ a_7)\cdots(a_{2k-2}\ a_{2k-1})(a_{2k}\ a_1) \end{array}\right\} \Longrightarrow$$

$$\Longrightarrow XY = (a_1\ a_3\ a_5\cdots a_{2k-3}\ a_{2k-1})(a_{2k}\ a_{2k-2}\cdots a_6\ a_4\ a_2)$$

Continuó la demostración añadiendo: *"Si, de este modo, no hemos agotado todas las letras de la permutación, continuaremos nuestro procedimiento hasta que lo hayamos hecho".*[6] ◇

Teorema 3.2.7 *Si una permutación de grado par consta de pares de ciclos disjuntos de la misma longitud, entonces esta permutación puede ser considerada como un producto de dos permutaciones, cada una compuesta exclusivamente de transposiciones disjuntas.*

Demostración. La demostración de este teorema es inmediata a partir de lo indicado anteriormente. Sea XY el producto de las permutaciones X e Y dado.
$XY = (a_1\ a_3; a_5\cdots a_{2k-3}\ a_{2k-1})(a_{2k}\ a_{2k-2}\cdots a_6\ a_4\ a_2) \Longrightarrow$

$$\Longrightarrow \left\{\begin{array}{l} X = (a_1\ a_2)(a_3\ a_4)(a_5\ a_6)\cdots(a_{2k-3}\ a_{2k-2})(a_{2k-1}\ a_{2k}) \\ Y = (a_2\ a_3)(a_4\ a_5)(a_6\ a_7)\cdots(a_{2k-2}\ a_{2k-1})(a_{2k}\ a_1) \end{array}\right.$$

◇

Rejewski señaló otros dos resultados que derivan de su demostración del Teorema 3.2.6.

Teorema 3.2.8 *Los elementos que forman parte de una única transposición, ya sea de la permutación X o de Y, siempre forman parte de dos ciclos distintos de la permutación XY.*

Teorema 3.2.9 *Si dos elementos que se encuentran en dos ciclos diferentes de la misma longitud de la permutación XY, pertenecen a la misma transposición, entonces los elementos adyacentes a ellos (uno a la derecha y el otro a la izquierda) también pertenecen a la misma transposición.*

[6] Extraído de: [2].

3.3. El conjunto de ecuaciones

Aunque no lo especificamos en su momento, al desarrollar las cadenas del Cuadro 3.1 estábamos formando ciclos. Hemos visto que dichos ciclos se pueden transformar en permutaciones, esto es, a partir de dicho cuadro podemos obtener permutaciones como productos de ciclos disjuntos. Tomamos el ejemplo del cuadro 3.1.

$$\mathtt{A} \longrightarrow \mathtt{F}; \quad \mathtt{F} \longrightarrow \mathtt{W}; \quad \mathtt{W} \longrightarrow \mathtt{A} \tag{3.1}$$

$$\begin{cases} \mathtt{B} \longrightarrow \mathtt{Q}; \quad \mathtt{Q} \longrightarrow \mathtt{Z}; \quad \mathtt{Z} \longrightarrow \mathtt{K}; \quad \mathtt{K} \longrightarrow \mathtt{V}; \quad \mathtt{V} \longrightarrow \mathtt{E}; \quad \mathtt{E} \longrightarrow \mathtt{L}; \\ \mathtt{L} \longrightarrow \mathtt{R}; \quad \mathtt{R} \longrightarrow \mathtt{I}; \quad \mathtt{I} \longrightarrow \mathtt{B} \end{cases} \tag{3.2}$$

$$\begin{cases} \mathtt{C} \longrightarrow \mathtt{H}; \quad \mathtt{H} \longrightarrow \mathtt{G}; \quad \mathtt{G} \longrightarrow \mathtt{O}; \quad \mathtt{O} \longrightarrow \mathtt{Y}; \quad \mathtt{Y} \longrightarrow \mathtt{D}; \quad \mathtt{D} \longrightarrow \mathtt{P}; \\ \mathtt{P} \longrightarrow \mathtt{C} \end{cases} \tag{3.3}$$

$$\begin{cases} \mathtt{J} \longrightarrow \mathtt{M}; \quad \mathtt{M} \longrightarrow \mathtt{X}; \quad \mathtt{X} \longrightarrow \mathtt{S}; \quad \mathtt{S} \longrightarrow \mathtt{T}; \quad \mathtt{T} \longrightarrow \mathtt{N}; \quad \mathtt{N} \longrightarrow \mathtt{U}; \\ \mathtt{U} \longrightarrow \mathtt{J} \end{cases} \tag{3.4}$$

De esta forma, obtenemos 4 ciclos: (A F W), correspondiente a 3.1; (B Q Z K V E L R I), correspondiente a 3.2; (C H G O Y D P), correspondiente a 3.3 y (J M X S T N U), correspondiente a 3.4. Nos interesa formar una permutación a partir del producto de ciclos disjuntos. Por lo que nuestra permutación, llamémosla P, sería $P = (\mathtt{A\ F\ W})(\mathtt{B\ Q\ Z\ K\ V\ E\ L\ R\ I})(\mathtt{C\ H\ G\ O\ Y\ D\ P})(\mathtt{J\ M\ X\ S\ T\ N\ U})$. Dicha permutación P representa la transformación de la primera letra en la cuarta.

El hecho de considerar la permutación P como una sola permutación y no como un producto de permutaciones ha sido un error por nuestra parte, ya que, como sabemos, Enigma cifra cada letra con una permutación diferente. Así, P en realidad sería un producto de dos permutaciones. Hemos de tener en cuenta que todas las primeras letras de las cabeceras de los mensajes han sido cifradas con la misma permutación, ya que la máquina parte siempre de la misma posición inicial indicada en la clave del día. Esto mismo ocurriría con las demás letras correspondientes a las cabeceras. De esta forma tendríamos la siguiente notación:

- Π_1: permutación que indica cómo cambian las letras cuando se pulsa una tecla por primera vez.

- Π_2: permutación que indica cómo cambian las letras cuando se pulsa una tecla por segunda vez.

⋮

- Π_6: permutación que indica cómo cambian las letras cuando se pulsa una tecla por sexta vez.

De esta forma, observamos que desconocemos las permutaciones[7] de la Π_1 a la Π_6, pero sí podríamos conocer las permutaciones $\Pi_4 \cdot \Pi_1$, $\Pi_5 \cdot \Pi_2$ y $\Pi_6 \cdot \Pi_3$.

Supongamos que tenemos como primera cabecera para un día determinado `ARWSJN`. Recordemos que las cabeceras son el resultado de cifrar dos veces tres letras desconocidas para el criptoanalista. Representemos con la letra `X` la primera de ellas. Deducimos, entonces, que Π_1 transforma `X` en `A` mientras que Π_4 sustituye `X` por `S`. Esto lo podríamos expresar del siguiente modo:

$$\Pi_1(\texttt{X}) = \texttt{A}$$
$$\Pi_4(\texttt{X}) = \texttt{S}$$

Recordemos ahora que el cifrado de Enigma tiene una propiedad denominada *reciprocidad*, es decir, se cumple que $A^{-1} = A$, $B^{-1} = B$, etc. En nuestro caso esto significa que si al pulsar `X` obtenemos `T`, entonces al pulsar `T` obtendremos `X`. Por lo tanto, tenemos $\Pi_1(\texttt{A}) = \texttt{X}$. Sustituyendo `X` en la otra igualdad: $\Pi_4(\Pi_1(\texttt{A})) = \texttt{S}$. Esto es, el producto $\Pi_4 \cdot \Pi_1$ transforma la letra `A` en `S`, es decir, $\Pi_4 \cdot \Pi_1(\texttt{A}) = \texttt{S}$. De la misma forma ocurrirá con las demás permutaciones. Así, obtenemos lo siguiente:

$$\begin{cases} \Pi_4 \cdot \Pi_1(\texttt{A}) = \texttt{S} \\ \Pi_5 \cdot \Pi_2(\texttt{R}) = \texttt{J} \\ \Pi_6 \cdot \Pi_3(\texttt{W}) = \texttt{N} \end{cases} \tag{3.5}$$

Por lo tanto, con solo el principio de los mensajes es posible obtener grandes avances para la desencriptación del código. Así, debido a la importancia de este hecho, Rejewski le prestó especial atención. Sustrajo las cabeceras de todos los mensajes de un mismo día y obtuvo listas como la que figura a continuación[8]. Los pasos a llevar acabo para obtener las cabeceras son los siguientes:

[7] Dichas permutaciones deben ser representadas como producto de ciclos disjuntos.

[8] Este conjunto se ha obtenido mediante el simulador de Enigma de la página *http://enigmaco.de/enigma/enigma_es.html*. La configuración inicial de la máquina ha sido la propuesta en el Cuadro 2.1 que se encuentra en la sección 3 del capítulo 2. Se propone para disfrute del lector averiguar el personaje mencionado en la lista de cabeceras. Para ello es necesario usar el simulador (con la configuración mencionada) y descifrar las tres primeras letras de cada cabecera.

1. Configurar Enigma de acuerdo al Cuadro 2.1.

2. Escribir tres letras al azar dos veces.

3. Volver a poner la máquina en la posición inicial[9] y repetir el procedimiento.

De esta forma, obtenemos el siguiente conjunto:

ARW SJN	JRL ZJR	MSM REG	AAH SIQ	IZR BDZ	ZPT MTM	TFH NXQ
BVA KCI	MOH RKQ	ARI SJV	JGC ZNP	WGW LNN	JKI ZGV	CCW EPN
MUC RQP	HTN WZD	MGC RNP	VFH XXQ	ZTN MZD	BGT KNM	CVC ECP
XRA YJI	MWQ RFF	JVM ZCG	DVT OCM	KIM DSG	DXK OWL	JDJ ZMO
CDT EMM	FMS CRT	CSH EEQ	OMZ TRU	NRK AJL	CKW EGN	JVO ZCB
JKM ZGG	XFV YXY	MSC REP	HTW WZN	MXH RWQ	ARL SJR	JRH ZJQ
RXM FWG	ZZX MDA	BVK KCL	MCQ RPF	DAW OIN	MIQ RSF	RST FEM
MXG RWK	FJH CYQ	OAB TIS	FTN CZD	CCT EPM	ORO TJB	PMH VRQ
QZA HDI	DVI OCV	ZTZ MZV	NZP ADH	YDD PMX	DRL OJR	EGC GNP
XXH YWQ	MCQ RPF	DDP OMH	DAF OIW	WAC LIP	SBO IHB	GMG URK
NZP ADH	MLB RUS	GQG ULK	LBF QHW	SND IBX	PEI VOV	QBD HHX
KOE DKJ	UAU JIE	GHQ UAF	YYY PVC	UAI JIV	XXN YWD	OGO TNB
EQQ GLF	IJR BYZ	WPS LTT	ZMX MRA	DVO OCB	JRM ZJG	CHQ EAF
DSQ OEF	XXN YWD	CPM ETG	TEE NOJ	NRN AJD	OGO TNB	AZL SDR

Cuadro 3.2: Lista de cabeceras.

Teniendo en cuenta las fórmulas de 3.5 y la tabla 3.2, podemos observar que disponemos de las suficientes cabeceras como para obtener completamente los productos de 3.5 (representados en el cuadro 3.3).

	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
$\Pi_4 \cdot \Pi_1$	S	K	E	O	G	C	U	W	B	Z	D	Q	R	A	T	V	H	F	I	N	J	X	L	Y	P	M
$\Pi_5 \cdot \Pi_2$	I	H	P	M	O	X	N	A	S	Y	G	U	R	B	K	T	L	J	E	Z	Q	C	F	W	V	D
$\Pi_6 \cdot \Pi_3$	I	S	P	X	J	W	K	Q	V	O	L	R	G	D	B	H	F	Z	T	M	E	Y	N	A	C	U

Cuadro 3.3: Los productos $\Pi_4 \cdot \Pi_1$, $\Pi_5 \cdot \Pi_2$ y $\Pi_6 \cdot \Pi_3$.

Procedemos ahora a factorizar los productos anteriores en ciclos disjuntos, recordando que el orden de los ciclos es indiferente debido a la conmutatividad de los ciclos disjuntos.

[9]Es necesario realizar este paso debido al giro del rotor derecho, el cual modifica la posición de dicho rotor con cada pulsación.

$$\Pi_4 \cdot \Pi_1 = (\texttt{A S I B K D O T N})(\texttt{C E G U J Z M R F})(\texttt{H W L Q})(\texttt{P V X Y})$$
$$\Pi_5 \cdot \Pi_2 = (\texttt{A I S E O K G N B H})(\texttt{C P T Z D M R J Y V})(\texttt{L U Q})(\texttt{W F X})$$
$$\Pi_6 \cdot \Pi_3 = (\texttt{A I V Y C P H Q F W N D X})(\texttt{J O B S T M G K L R Z U E})$$

En las tres factorizaciones anteriores aparecen pares de ciclos de igual longitud. Esto ya se sabía gracias al Teorema 3.2.7, por lo que deducimos que los tres productos consisten en trece transposiciones disjuntas. Además, Rejewski, con su demostración, indicó la forma de encontrar dichas transposiciones. Explicamos el procedimiento a seguir fijándonos, por ejemplo, en el producto $\Pi_6 \cdot \Pi_3$. Observamos que hay dos ciclos de la misma longitud. Elegimos una letra en cada ciclo y escribimos los ciclos uno debajo del otro, empezando por las letras elegidas y ordenando las letras de uno de ellos en modo inverso. Seleccionamos, por ejemplo, las letras `H` y `K`, tenemos entonces:

$$(\texttt{H Q F W N D X A I V Y C P})$$
$$(\texttt{K G M T S B O J E U Z R L})$$

Ahora, las dos letras de cada columna determinan transposiciones del segundo factor y las diagonales ascendentes proporcionan transposiciones del primer factor. Esto es:

$$\Pi_3 : (\texttt{H K}), (\texttt{Q G}), (\texttt{F M}), (\texttt{W T}), ..., (\texttt{P L})$$
$$\Pi_6 : (\texttt{K Q}), (\texttt{G F}), (\texttt{M W}), (\texttt{T N}), ..., (\texttt{L H})$$

Al realizar la descomposición vemos que existen varias soluciones para cada uno de los factores buscados, ya que, variando las letras elegidas obtendremos resultados diferentes. ¿Cómo resolver el problema?

Rejewski observó que, entre las decenas de mensajes que los alemanes se transmitían diariamente, era frecuente encontrar cabeceras repetidas. Este hecho le provocó confusión. Teniendo en cuenta que hay $26^3 = 17576$ tríos de letras para escoger es inusual que algún trío se repita en un mismo día. Por tanto, Rejewski pensó que eso se debía al hecho de que algunos operadores elegían ternas con las tres letras iguales[10].

Observando el cuadro 3.2 podemos encontrar fragmentos que se repiten. Ellos son: `XXNYWD` y `OGOTNB`. Suponiendo que hemos seguido fielmente el modo de proceder de los operadores alemanes, podemos sospechar que estos fragmentos provienen de tríos de letras iguales. Veamos, entonces, el método para hallar dichas letras.

[10]Como solo hay 26 distintas, es fácil que se produzcan repeticiones.

1. Consideremos primero XXNYWD. Una letra que mediante Π_1 se transforme en X debe estar en el ciclo de $\Pi_4 \cdot \Pi_1$ que se empareja con el que contiene dicha X. Ese ciclo es (H W L Q). De la misma forma, una letra que mediante Π_2 se transforme en X debe estar en el ciclo (L U Q). Análogamente, una letra que mediante Π_3 se transforme en N debe estar en el ciclo (J O B S T M G K L R Z U E). Estos tres ciclos tienen únicamente una letra en común: L. Por lo tanto, XXNYWD ha sido originada por la terna LLL.

2. Consideremos ahora OGOTNB. Procediendo del mismo modo que en el caso anterior, los tres ciclos que obtendríamos son: (C E G U J Z M R F), (C P T Z D M R J Y V) y (A I V Y C P H Q F W N D X). La única letra que tienen en común es la C. Por lo tanto, OGOTNB ha sido originada por la terna CCC.

Para aplicar el método que describimos para obtener las trece transposiciones disjuntas y para que esta descomposición sea única, necesitamos comenzar con un producto que esté únicamente compuesto por dos ciclos de longitud trece[11]. Para comenzar, centraremos nuestra atención en el producto $\Pi_6 \cdot \Pi_3$, el cual cumple dichas condiciones.

Tenemos entonces: $\Pi_3(\mathtt{C}) = \mathtt{O}$. Este dato permite ya determinar tanto Π_3 como Π_6. Para obtener sus trece transposiciones disjuntas, procedemos según explicamos anteriormente: asociamos ahora la O con la C y escribimos de nuevo los dos ciclos de longitud trece de $\Pi_6 \cdot \Pi_3$, uno debajo del otro y con las letras del segundo en orden inverso:

$$(\mathtt{O\ B\ S\ T\ M\ G\ K\ L\ R\ Z\ U\ E\ J})$$
$$(\mathtt{C\ Y\ V\ I\ A\ X\ D\ N\ W\ F\ Q\ H\ P})$$

Entonces:

$$\Pi_3 = (\mathtt{O\ C})(\mathtt{B\ Y})(\mathtt{S\ V})(\mathtt{T\ I})(\mathtt{M\ A})(\mathtt{G\ X})(\mathtt{K\ D})(\mathtt{L\ N})(\mathtt{R\ W})(\mathtt{Z\ F})(\mathtt{U\ Q})(\mathtt{E\ H})(\mathtt{J\ P})$$
$$\Pi_6 = (\mathtt{C\ B})(\mathtt{Y\ S})(\mathtt{V\ T})(\mathtt{I\ M})(\mathtt{A\ G})(\mathtt{X\ K})(\mathtt{D\ L})(\mathtt{N\ R})(\mathtt{W\ Z})(\mathtt{F\ U})(\mathtt{Q\ E})(\mathtt{H\ J})(\mathtt{P\ O})$$

Emparejamos ahora la O con la C con el fin de obtener $\Pi_4 \cdot \Pi_1$. Observamos que, de esta forma, solo podemos obtener 9 transposiciones[12]. Para calcular las otras cuatro, necesitaríamos emparejar letras de los otros dos ciclos. Consideremos otra vez la cabecera repetida XXNYWD. De aquí se deduce: $\Pi_1(\mathtt{L}) = \mathtt{X}$.

[11] También se podría realizar si tuviésemos dos ciclos de igual longitud y los demás ciclos de longitud 1.

[12] 9 es la longitud de los dos ciclos que contienen a O y C.

Por lo tanto, ya tenemos el emparejamiento que nos faltaba: L con X. Solo nos falta escribir convenientemente los ciclos de $\Pi_4 \cdot \Pi_1$ y, de ahí, obtener Π_1 y Π_4.

$$\begin{array}{ll} (\texttt{O T N A S I B K D}) & (\texttt{L Q H W}) \\ (\texttt{C F R M Z J U G E}) & (\texttt{X V P Y}) \end{array}$$

Entonces:

$$\Pi_1 = (\texttt{O C})(\texttt{T F})(\texttt{N R})(\texttt{A M})(\texttt{S Z})(\texttt{I J})(\texttt{B U})(\texttt{K G})(\texttt{D E})(\texttt{L X})(\texttt{Q V})(\texttt{H P})(\texttt{W Y})$$
$$\Pi_4 = (\texttt{C T})(\texttt{F N})(\texttt{R A})(\texttt{M S})(\texttt{Z I})(\texttt{J B})(\texttt{U K})(\texttt{G D})(\texttt{E O})(\texttt{X Q})(\texttt{V H})(\texttt{P W})(\texttt{Y L})$$

En el caso del producto $\Pi_5 \cdot \Pi_2$ ocurre algo parecido a lo anterior. Ahora solo podremos obtener 10 transposiciones emparejando g con c. Para calcular las otras tres, necesitaríamos emparejar letras de los otros dos ciclos. Consideremos nuevamente la cabecera repetida XXNYWD. De aquí se deduce: $\Pi_2(\texttt{L}) = \texttt{X}$. Por lo tanto, ya tenemos el emparejamiento que nos faltaba: l con x. Solo nos falta escribir convenientemente los ciclos de $\Pi_5 \cdot \Pi_2$ y, de ahí, obtener Π_2 y Π_5.

$$\begin{array}{ll} (\texttt{G N B H A I S E O K}) & (\texttt{L U Q}) \\ (\texttt{C V Y J R M D Z T P}) & (\texttt{X F W}) \end{array}$$

Entonces:

$$\Pi_2 = (\texttt{G C})(\texttt{N V})(\texttt{B Y})(\texttt{H J})(\texttt{A R})(\texttt{I M})(\texttt{S D})(\texttt{E Z})(\texttt{O T})(\texttt{K P})(\texttt{L X})(\texttt{U F})(\texttt{Q W})$$
$$\Pi_5 = (\texttt{C N})(\texttt{V B})(\texttt{Y H})(\texttt{J A})(\texttt{R I})(\texttt{M S})(\texttt{D E})(\texttt{Z O})(\texttt{T K})(\texttt{P G})(\texttt{X U})(\texttt{F Q})(\texttt{W L})$$

Una vez calculadas las permutaciones Π_i de un cierto día, es posible recuperar todas las claves de ese día. Veamos, por ejemplo, cuál es la terna que dio lugar a la primera cabecera de nuestra lista: ARWSJN. Tenemos que $\Pi_1(\texttt{A}) = \texttt{M}$, $\Pi_2(\texttt{R}) = \texttt{A}$ y $\Pi_3(\texttt{W}) = \texttt{R}$. Por lo tanto, dicha terna es MAR.

Así, el primer paso hacia el criptoanálisis de Enigma ya estaba dado, gracias al doble cifrado de las claves. Sin embargo, el hecho de conocer las claves no sirve relativamente de nada, ya que para poder descifrar los mensajes se necesitaba un ejemplar de la máquina con las mismas conexiones internas que las que usaban los alemanes. No obstante, a Rejewski no le hizo falta disponer de dicha máquina, puesto que supo cómo deducir las conexiones de los rotores.

La reconstrucción del cableado

Como podemos observar, con el razonamiento anterior, solo estamos teniendo en cuenta en nuestro estudio la parte correspondiente a los rotores. Sin embargo, Rejewski supo vislumbrar que todo el mecanismo de Enigma podía ser representado con permutaciones. Recordemos el funcionamiento de la máquina: el operario pulsaba una tecla, entonces la señal eléctrica pasaba primero por el clavijero, donde algunas letras eran intercambiadas, produciéndose así la primera permutación; después seguía su camino hasta el cilindro de entrada, donde se producía la segunda; a continuación, la señal eléctrica llegaba a los rotores, pasando por ellos de derecha a izquierda y, por último, dicha señal rebotaba en el reflector e invertía el orden de su camino, iluminándose la correspondiente letra cifrada en el panel de luces. Así, podemos representar el recorrido de la señal eléctrica como el producto de las siguientes permutaciones:

- S: permutación causada por el clavijero.
- E: permutación causada por el cilindro de entrada.
- N: permutación causada por el rotor derecho.
- M: permutación causada por el rotor central.
- L: permutación causada por el rotor izquierdo.
- R: permutación causada por el reflector.

De esta forma, podemos expresar el recorrido de la señal eléctrica tanto en su camino de ida como de vuelta.

- Camino de ida: $SENMLR$
- Camino de vuelta: $(S\ E\ N\ M\ L)^{-1} = L^{-1}M^{-1}N^{-1}E^{-1}S^{-1}$

Cabe señalar que el camino de vuelta es casi la inversa del recorrido de ida, con la excepción de la permutación debida al reflector, que es donde se conectan los dos caminos. Por lo tanto, el efecto de pulsar una tecla se representa mediante la permutación:

$$SENMLRL^{-1}M^{-1}N^{-1}E^{-1}S^{-1} = (S\ E\ N\ M\ L)R(S\ E\ N\ M\ L)^{-1}$$

Debido a que los alemanes utilizaron el mismo tipo de reflector para todos los modelos de Enigma, se pudo conocer el resultado de la permutación causada por este:

$$R = (\texttt{A E})(\texttt{B J})(\texttt{C M})(\texttt{D Z})(\texttt{F L})(\texttt{G Y})(\texttt{H X})(\texttt{I V})(\texttt{K W})(\texttt{N R})(\texttt{O P})(\texttt{P U})(\texttt{S T})$$

Otro hecho a tener en cuenta es el giro del rotor derecho. Únicamente tras el giro de dicho rotor se cerraba el circuito eléctrico. Para tomar en cuenta este movimiento debemos introducir una nueva permutación especial de un ciclo que transforma cada letra del alfabeto en la siguiente; la designaremos con la letra P:

$$P = (\texttt{A B C D E F G H I J K L M N O P Q R S T U V W X Y Z})$$

De esta forma, podemos decir que cuando el rotor derecho gira, se produce la permutación P, luego la N y después la inversa de P, es decir, PNP^{-1}. En el camino de vuelta, la permutación será la inversa de la anterior, es decir, $P^{-1}N^{-1}P$. Al pulsar por segunda vez una tecla, con el correspondiente giro del rotor, se produce la permutación $P^2NP^{-2} = PPNP^{-1}P^{-1}$ a la ida y $P^{-2}N^{-1}P^2$ a la vuelta.

La siguiente figura[13] nos permite seguir el recorrido de la corriente eléctrica antes y después del movimiento del rotor N.

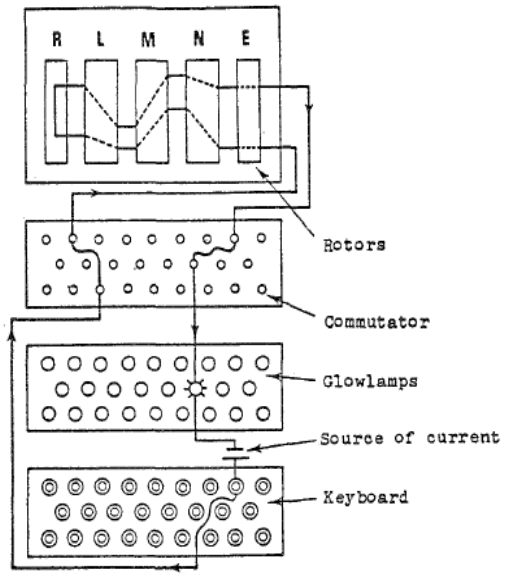


Figura 3.1: Recorrido de la corriente eléctrica a través de los componentes de Enigma.

Observando la Figura 3.1, parece evidente que las permutaciones desconocidas Π_1 hasta Π_6 puedan ser representadas de la siguiente forma:

[13] **Aclaraciones:** • *Rotors*: Rotores (en este conjunto se incluyen el reflector, los tres rotores y el cilindro de entrada; • *Commutator*: Clavijero; • *Glowlamps*: Panel de luces; • *Source of current*: Fuente de corriente; • *Keyboard*: Teclado.

$$\begin{aligned}\Pi_1 &= SEPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}E^{-1}S^{-1}\\ &= (S\ E\ P\ N\ P^{-1}\ M\ L)R(S\ E\ P\ N\ P^{-1}\ M\ L)^{-1}\end{aligned}$$

$$\begin{aligned}\Pi_2 &= SEP^2NP^{-2}MLRL^{-1}M^{-1}P^2N^{-1}P^{-2}E^{-1}S^{-1}\\ &= (S\ E\ P^2\ N\ P^{-2}\ M\ L)R(S\ E\ P^2\ N\ P^{-2}\ M\ L)^{-1}\end{aligned}$$

$$\begin{aligned}\Pi_3 &= SEP^3NP^{-3}MLRL^{-1}M^{-1}P^3N^{-1}P^{-3}E^{-1}S^{-1}\\ &= (S\ E\ P^3\ N\ P^{-3}\ M\ L)R(S\ E\ P^3\ N\ P^{-3}\ M\ L)^{-1}\end{aligned}$$

$$\begin{aligned}\Pi_4 &= SEP^4NP^{-4}MLRL^{-1}M^{-1}P^4N^{-1}P^{-4}E^{-1}S^{-1}\\ &= (S\ E\ P^4\ N\ P^{-4}\ M\ L)R(S\ E\ P^4\ N\ P^{-4}\ M\ L)^{-1}\end{aligned}$$

$$\begin{aligned}\Pi_5 &= SEP^5NP^{-5}MLRL^{-1}M^{-1}P^5N^{-1}P^{-5}E^{-1}S^{-1}\\ &= (S\ E\ P^5\ N\ P^{-5}\ M\ L)R(S\ E\ P^5\ N\ P^{-5}\ M\ L)^{-1}\end{aligned}$$

$$\begin{aligned}\Pi_6 &= SEP^6NP^{-6}MLRL^{-1}M^{-1}P^6N^{-1}P^{-6}E^{-1}S^{-1}\\ &= (S\ E\ P^6\ N\ P^{-6}\ M\ L)R(S\ E\ P^6\ N\ P^{-6}\ M\ L)^{-1}\end{aligned}$$

La primera parte de nuestra tarea consiste esencialmente en resolver este conjunto de ecuaciones. Para ello, debemos conocer S, E, N, M, L y R, ya que de este modo podríamos averiguar la configuración del cableado de los rotores y el reflector. Al ser estas permutaciones desconocidas, el conjunto es sin duda irresoluble. Por lo tanto, buscaremos simplificarlo. El primer paso es puramente formal y consiste en reemplazar el producto repetido $MLRL^{-1}M^{-1}$ por una sola letra Q; de este modo quedan reducidas temporalmente el número de incógnitas a 4, las denominadas E, S, N y Q. Así, tenemos:

$$\left.\begin{aligned}\Pi_1 &= SEPNP^{-1}QPN^{-1}P^{-1}E^{-1}S^{-1}\\ \Pi_2 &= SEP^2NP^{-2}QP^2N^{-1}P^{-2}E^{-1}S^{-1}\\ \Pi_3 &= SEP^3NP^{-3}QP^3N^{-1}P^{-3}E^{-1}S^{-1}\\ \Pi_4 &= SEP^4NP^{-4}QP^4N^{-1}P^{-4}E^{-1}S^{-1}\\ \Pi_5 &= SEP^5NP^{-5}QP^5N^{-1}P^{-5}E^{-1}S^{-1}\\ \Pi_6 &= SEP^6NP^{-6}QP^6N^{-1}P^{-6}E^{-1}S^{-1}\end{aligned}\right\}\Longrightarrow$$

$$\Longrightarrow\begin{cases}\Pi_4\cdot\Pi_1 = SEPNP^{-1}QPN^{-1}P^3NP^{-4}QP^4N^{-1}P^{-4}E^{-1}S^{-1}\\ \Pi_5\cdot\Pi_2 = SEP^2NP^{-2}QP^2N^{-1}P^3NP^{-5}QP^5N^{-1}P^{-5}E^{-1}S^{-1}\\ \Pi_6\cdot\Pi_3 = SEP^3NP^{-3}QP^3N^{-1}P^3NP^{-6}QP^6N^{-1}P^{-6}E^{-1}S^{-1}\end{cases}$$

Llegado a este punto, Rejewski no conocía aún siquiera si la ecuaciones que dan Π_1, Π_2, Π_3, Π_4, Π_5 y Π_6 resultaban ser despejables para obtener S, E, N y Q. Dichas ecuaciones podrían ser resueltas si dispusiéramos de mensajes de dos días diferentes, en los cuales las conexiones del clavijero fuesen diferentes, pero los rotores estuvieran en las mismas posiciones. Algo que era muy poco probable que ocurriese.

Es aquí cuando tuvo importancia la aparición del espía alemán Hans Thilo Schmidt, del que hablamos en el primer capítulo. Fue en este momento cuando Rejewski se apoyó en los documentos proporcionados por Hans. Así, además de las permutaciones $\Pi_4 \cdot \Pi_1$, $\Pi_5 \cdot \Pi_2$ y $\Pi_6 \cdot \Pi_3$ (obtenidas mediante radioescucha) y las Π_1, Π_2, Π_3, Π_4, Π_5 y Π_6 (deducidas por los criptoanalistas polacos), ahora se conocían también las permutaciones S y E (esta última se dio por supuesta). De esta forma tenemos ahora[14]:

$$\begin{cases} E^{-1}S^{-1}ASE = PNP^{-1}QPN^{-1}P^{-1} \\ E^{-1}S^{-1}BSE = P^2NP^{-2}QP^2N^{-1}P^{-2} \\ E^{-1}S^{-1}CSE = P^3NP^{-3}QP^3N^{-1}P^{-3} \\ E^{-1}S^{-1}DSE = P^4NP^{-4}QP^4N^{-1}P^{-4} \\ E^{-1}S^{-1}ESE = P^5NP^{-5}QP^5N^{-1}P^{-5} \\ E^{-1}S^{-1}FSE = P^6NP^{-6}QP^6N^{-1}P^{-6} \end{cases}$$

Ahora solo tenemos las incógnitas N y Q. Por lo tanto, definimos ahora nuevas permutaciones, denominadas U, V, W, W, Y y Z, del siguiente modo:

$$\begin{cases} U = P^{-1}E^{-1}S^{-1}ASEP & = NP^{-1}QPN^{-1} \\ V = P^{-1}E^{-1}S^{-1}BSEP & = NP^{-2}QP^2N^{-1} \\ W = P^{-1}E^{-1}S^{-1}CSEP & = NP^{-3}QP^3N^{-1} \\ X = P^{-1}E^{-1}S^{-1}DSEP & = NP^{-4}QP^4N^{-1} \\ Y = P^{-1}E^{-1}S^{-1}ESEP & = NP^{-5}QP^5N^{-1} \\ Z = P^{-1}E^{-1}S^{-1}FSEP & = NP^{-6}QP^6N^{-1} \end{cases}$$

Una vez obtenidas estas permutaciones, Rejewski calculó las permutaciones compuestas UV, VW, WX, XY e YZ, resultando:

[14] Multiplicando Π_1, Π_2, Π_3, Π_4, Π_5 y Π_6 por:

- $E^{-1}S^{-1}$ por la izquierda.
- SE por la derecha.

$$\begin{cases} UV = NP^{-1}(QP^{-1}QP)PN^{-1} \\ VW = NP^{-2}(QP^{-1}QP)P^2N^{-1} \\ WX = NP^{-3}(QP^{-1}QP)P^3N^{-1} \\ XY = NP^{-4}(QP^{-1}QP)P^4N^{-1} \\ YZ = NP^{-5}(QP^{-1}QP)P^5N^{-1} \end{cases}$$

Ahora, despejando $(QP^{-1}QP)$ de una de las ecuaciones anteriores e introduciéndolo en las otras, obtenemos:

$$\begin{cases} VW = NP^{-1}N^{-1}UVNPN^{-1} \\ WX = NP^{-1}N^{-1}VWNPN^{-1} \\ XY = NP^{-1}N^{-1}WXNPN^{-1} \\ YZ = NP^{-1}N^{-1}WYNPN^{-1} \end{cases}$$

donde la única incógnita es la permutación NPN^{-1}. Así, para un mismo día se podrían obtener decenas de soluciones para VW, WX, XY e YZ, todas con una estructura común. Además, empleando el método usado para obtener Π_1, Π_2, Π_3, Π_4, Π_5 y Π_6 partiendo de los productos $\Pi_4 \cdot \Pi_1$, $\Pi_5 \cdot \Pi_2$ y $\Pi_6 \cdot \Pi_3$, podemos determinar NPN^{-1} partiendo de WX, obteniendo también distintas soluciones. También podemos obtener varias soluciones a partir de WX, y únicamente existe solución idéntica para VW y WX. Del mismo modo, se puede obtener N a partir de NPN^{-1}. Para ello basta con aplicar una de las 26 permutaciones P que existen para obtener N[15].

Todo este estudio fue un logro. Sin embargo, Rejewski tuvo un error al principio de su estudio, el hecho de considerar la permutación E conocida, es decir, la suposición de que dicha permutación era la misma que la de la Enigma comercial. No obstante, una vez más, Rejewski supo resolver este problema. Consideró E como la permutación alfabética. Esto es, supuso que las teclas se unirían mediante cables al cilindro de entrada siguiendo el orden `ABCDE...`. Una vez supuesto esto, Rejewski lo probó, obteniendo gran éxito al resultar correcta dicha hipótesis.

A todo este estudio debemos añadir dos complicaciones más. Rejewski no había tenido en cuenta hasta ahora que no solo el rotor derecho giraba con cada pulsación, sino que también lo hacían, en intervalos menos frecuentes, los rotores central e izquierdo. Además, hay que sumar el hecho de que el orden de estos rotores podía ser cambiado.

[15]Parece apropiado mostrar cómo los resultados teóricos anteriores se aplican en la práctica para obtener las conexiones internas del rotor N. Un ejemplo de ello lo podemos encontrar en [6].

Esta última complicación lleva una implicación no prevista por los diseñadores de Enigma: era frecuente localizar a cada uno de los tres rotores en la posición derecha. Como resultado a esto, el método anteriormente descrito para reconstruir la permutación N debía ser ampliado, teniendo en cuenta el giro para cada rotor. Por lo tanto, la estructura interior de la máquina tendría que ser reconstruida completamente.

Capítulo 4

El ataque, propiamente dicho

La reconstrucción de la máquina era una condición necesaria, pero no suficiente, para llevar a cabo la desencriptación del código. También era necesario hallar métodos que permitiesen reconstruir las claves diarias con rapidez. Así pues, llegados a este punto, el trabajo de los criptoanalistas se centraría en ese objetivo.

4.1. La característica

Todo el análisis propuesto en el capítulo anterior parte de los productos $\Pi_4 \cdot \Pi_1$, $\Pi_5 \cdot \Pi_2$, $\Pi_6 \cdot \Pi_3$. Analizándolo, 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[1]. Rejewski denominó *característica* a dicho número de ciclos y longitudes.

Ejemplo. Veamos cuál es la característica del ejemplo propuesto en la sección 3.3.

$$\left.\begin{aligned} \Pi_4 \cdot \Pi_1 &= (\texttt{A S I B K D O T N})(\texttt{C E G U J Z M R F})(\texttt{H W L Q})(\texttt{P V X Y}) \\ \Pi_5 \cdot \Pi_2 &= (\texttt{A I S E O K G N B H})(\texttt{C P T Z D M R J Y V})(\texttt{L U Q})(\texttt{W F X}) \\ \Pi_6 \cdot \Pi_3 &= (\texttt{A I V Y C P H Q F W N D X})(\texttt{J O B S T M G K L R Z U E}) \end{aligned}\right\} \Longrightarrow$$

$\Longrightarrow$ La característica es: $\{9, 9, 4, 4\}, \{10, 10, 3, 3\}$ y $\{13, 13\}$

Gracias a la no influencia del clavijero y, tal y como dedujimos en el capítulo anterior, el número de características a calcular pasaría a ser $6 \times 26^3 = 105456$,

[1] Este hecho ya lo adelantamos en la sección 3.1.

una para cada orden de los rotores y cada posición inicial de estos. Con esto se redujo en gran medida el trabajo a realizar. Sin embargo, calcular tal cantidad de características llevaría muchísimo tiempo. Es en este momento cuando Rejewski decide pedir ayuda a sus dos compañeros, Zygalski y Ròżycki. No obstante, aún contando con la inestimable ayuda de estos, dicho trabajo seguía siendo desmesurado. Llegados a este punto, los ingenieros polacos decidieron intervenir.

Ingeniería polaca

Con el fin de mecanizar el cálculo de las características, cuatro ingenieros polacos[2] construyeron, con la más absoluta confidencialidad, quince réplicas de la Enigma militar. Aún con la mecanización del cálculo, el trabajo se llevaría a cabo de forma prácticamente manual.

Recordemos que los tres rotores se pueden colocar en la máquina de seis formas diferentes y estos pueden asumir $26^3 = 17576$ posiciones diferentes. Así, la tarea de los operarios consistiría en girar los rotores con las distintas posibilidades y obtener de esta forma la configuración inicial de la máquina. Dicha tarea conlleva un gran trabajo por parte de los operarios, ya que el número de veces que debían teclear para obtener su objetivo resultó ser desorbitado. Rejewski intentó buscar una solución a este problema diseñando un dispositivo que facilitara el trabajo al que denominó *ciclómetro*.

El ciclómetro

El ciclómetro era una máquina Enigma doble, es decir, estaba compuesto por seis rotores (en lugar de tres) y dos reflectores (en lugar de uno). Sin embargo, el segundo conjunto de rotores estaba dispuesto de una forma especial. El efecto que se consiguió con el ciclómetro fue el mismo que si se pulsase, en una máquina convencional, una tecla, después dos y luego la misma otra vez. El trabajo quedó considerablemente reducido, ya que ahora los operarios solo necesitaban teclear una vez en lugar de cuatro. La Figura 4.1[3] dará una idea general de la apariencia de este artilugio.

La parte principal del ciclómetro está comprendida por los dos conjuntos de rotores, adecuadamente conectados por cables a través de los cuales circula la

[2]Antoni Palluth, Edward Fockczyński y los hermanos Ludomir y Leonard Danilewicz, directores de la compañía de Radiomanufactura AVA, encargada de diseñar y construir equipos de radio para abastecer al Biuro Szyfrów.

[3]**Aclaraciones:** • *Rotor lid closed*: Tapa del rotor cerrada; • *Rotor lid open*: Tapa del rotor abierta; • *Glowlamps*: Panel de luces; • *Switches*: Interruptores; • *Letters*: Letras; • *Rheostat*: Reóstato (Componente eléctrico usado para regular la intensidad de la corriente sin necesidad de abrir el circuito. Consiste en una resistencia eléctrica que puede variarse a nuestra conveniencia).

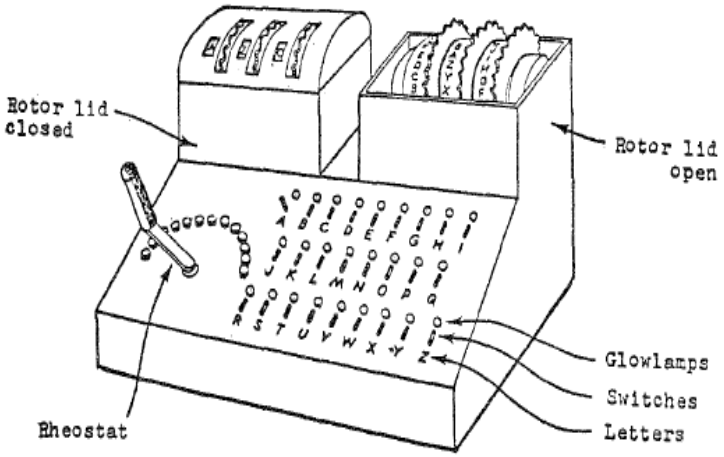


Figura 4.1: Ciclómetro.

corriente eléctrica. Como adelantábamos, la disposición del segundo conjunto era especial. El rotor derecho de este último estaba desplazado tres posiciones 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 Figura 4.2[4] está representado el funcionamiento del ciclómetro. Al accionar una palanca[5], la corriente eléctrica atraviesa varias veces el conjunto de rotores hasta iluminar un número par de letras, las correspondientes a dos ciclos asociados de la permutación $\Pi_4 \cdot \Pi_1$. Tras encenderse la luz correspondiente a una letra no iluminada hasta ahora, procedemos a pulsar un interruptor diferente. Esto provoca que otras letras se iluminen. Dichas letras determinan otro par de ciclos asociados. Así, se determinaba la descomposición en ciclos disjuntos de $\Pi_4 \cdot \Pi_1$. Procediendo del mismo modo, variando el orden de los rotores y sus posiciones iniciales, se obtienen todas las permutaciones $\Pi_4 \cdot \Pi_1$ existentes. Esto fue suficiente para calcular todas las características, ya que las permutaciones $\Pi_5 \cdot \Pi_2$ y $\Pi_6 \cdot \Pi_3$ asociadas a una determinada posición de los rotores coincidicen con la $\Pi_4 \cdot \Pi_1$ obtenida tras adelantar los rotores de la derecha del ciclómetro una o dos posiciones, respectivamente.

Una vez obtenidas, Rejewski las compiló en lo que denominó *catálogo de características*. En dicho catálogo aparecía cada característica y, a continua-

[4]**Aclaraciones:** • Para mayor claridad, el orden de los rotores del segundo conjunto ha sido invertido (esto no altera la parte esencial del estudio). • Los reflectores han sido designados con la letra Q, reemplazando en este dibujo a los rotores central e izquierdo y al reflector original. • El rotor derecho ha sido designado con la letra N. • Entre los dos conjuntos de rotores se encuentra el panel de luces.

[5]El ciclómetro disponía de 26 palancas, correspondientes a cada una de las letras del alfabeto.

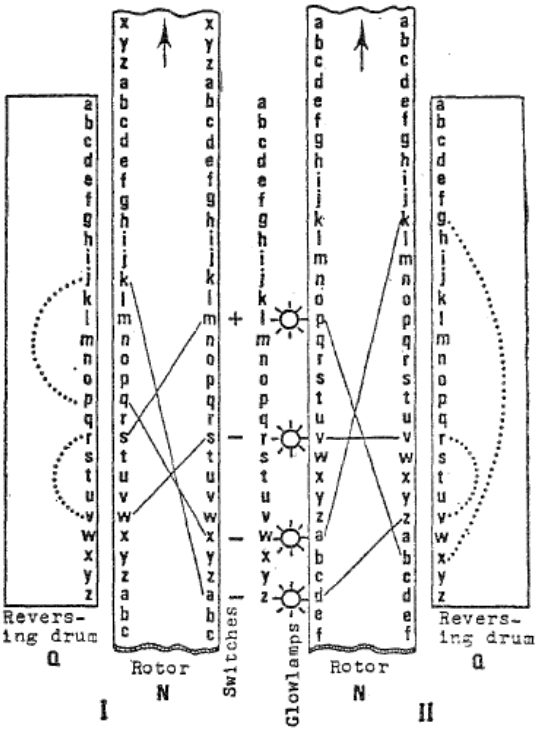


Figura 4.2: Diagrama del ciclómetro.

ción, el correspondiente orden de los rotores y sus posiciones iniciales. De esta forma, con cada mensaje que se interceptaba bastaba acudir al catálogo para encontrar la disposición de los rotores de un día determinado.

Aunque el ciclómetro fue un gran invento y se pudo disponer de varios de ellos, completar el catálogo implicó el trabajo de muchos operarios durante un largo periodo de tiempo. A esto hay que añadir que la modificación de la Enigma militar llevada a cabo por los alemanes implicó la construcción de un nuevo catálogo[6]. Esto, unido a una nueva modificación de la máquina, supuso el fin del uso del ciclómetro.

"Female"

Los nuevos cambios introducidos consistían básicamente en la libre elección, por parte del operador, de las claves de cada mensaje y la configuración inicial de los rotores. Estas variaciones dejaron inservibles todos los métodos de desencriptación efectuados hasta el momento[7].

[6]Cambiaron el cableado del reflector. Como sabemos, esto no influía apenas en el estudio realizado por Rejewski.

[7]Ya no había productos $\Pi_4 \cdot \Pi_1$, $\Pi_5 \cdot \Pi_2$, $\Pi_6 \cdot \Pi_3$, característicos para cada día, cuya configuración pudiera ser encontrada en el catálogo.

A partir de entonces, se procedería de la siguiente forma:

1. Las tres letras correspondientes al *Grundstellung* (distinto en cada uno de los mensajes, pero conocido) se transmitirían en claro en la cabecera del mensaje.

2. Las seis letras resultantes del doble cifrado de la *Spruchschlüssel* (indescifrable) irían seguidas de las anteriores.

De esta forma, la cabecera del mensaje pasaría a estar formada por nueve letras. Un ejemplo[8] podría ser: `DEO LTVQJX`, donde `DEO` indica la posición inicial de los rotores y `LTVQJX` el doble cifrado de la clave del mensaje. El resto del proceso de cifrado no sufrió ninguna variación, por lo que los polacos podrían seguir valiéndose del mayor error cometido por los alemanes hasta el momento: el doble cifrado de la *Spruchschlüssel*.

Recordemos que el objetivo perseguido por Rejewski era conseguir la elaboración del catálogo de características. Para ello tuvieron que calcular los 105456 productos de $\Pi_4 \cdot \Pi_1$[9]. Una vez calculados pudieron comprobar que el 40 % de estas permutaciones contenían ciclos de longitud 1. Dichos ciclos se manifiestan en las cabeceras de los mensajes mediante reiteraciones en las letras que siguen al *Grundstellung*. Esto es, en el segundo conjunto de la cabecera se producían repeticiones de algunos caracteres en idénticas posiciones. A dichas repeticiones se las designó con el término *female*.

Ejemplo.[10] Con una cantidad suficiente de material cifrado era posible encontrar cabeceras como las siguientes:

```
RTJ WAHWIK
DQY DWJMWR
HPN RAWKTW
```

donde la primera y la cuarta, la segunda y la quinta o la tercera y la sexta letra de la claves de los tres mensajes eran la misma. En este caso, esa letra es la `W`, ya que es la misma en los tres mensajes, pero podría ser cualquier otra. El mensaje con la cabecera `RTJ WAHWIK` indica que la permutación $\Pi_4 \cdot \Pi_1$ correspondiente contiene el ciclo `W` y usando la terminología empleada por los criptoanalistas se trataría de una 1,4-*female*; el de la cabecera `DQY DWJMWR` indica que la permutación $\Pi_5 \cdot \Pi_2$ contiene el ciclo (`W`) y se trataría de una 2,5-*female*; y el de la cabecera `HPN RAWKTW` indica que la permutación $\Pi_6 \cdot \Pi_3$ contiene el ciclo (`W`) y se trataría de una 3,6-*female*.

Si en el anterior ejemplo suponemos:

[8] Extraído de la sección 2.3.1.

[9] Tal y como explicamos anteriormente las permutaciones $\Pi_5 \cdot \Pi_2$ y $\Pi_6 \cdot \Pi_3$ asociadas a una determinada posición de los rotores coindicen con las $\Pi_4 \cdot \Pi_1$ de otras posiciones.

[10] Extraído de: [5].

1. La permutación S es la identidad.
2. La distribución inicial de los anillos de los rotores es la misma.
3. Conocemos el orden en el que se establen los rotores.

entonces bastaría con establecer los rotores en la posición `RTJ` y, a continuación, pulsar tres veces seguidas la tecla `W`. Así, la misma luz se encendería. Lo mismo ocurriría con las posiciones `DQY` y `HPN`. De esta forma, podemos ver que el ajuste de los anillos hace que las posiciones de los rotores pasen a ser desconocidas. Sin embargo, las diferencias en las posiciones se mantendrán y, por tanto, pasarán a ser conocidas.

Gracias a lo deducido anteriormente, podemos concluir que, como la longitud de los ciclos en las permutaciones $\Pi_4 \cdot \Pi_1$, $\Pi_5 \cdot \Pi_2$, $\Pi_6 \cdot \Pi_3$ es invariable respecto a las transformaciones producidas por la permutación S, la aparición o no aparición de *female* en los productos era invariable respecto a estas transformaciones.

Recordemos que el objetivo fundamental del trabajo criptológico consistía principalmente en identificar correctamente el orden de cada uno de los rotores y la configuración del anillo entre las 105456 posibles configuraciones. Dado que el 40 % de las permutaciones $\Pi_4 \cdot \Pi_1$, $\Pi_5 \cdot \Pi_2$, $\Pi_6 \cdot \Pi_3$ contiene ciclos de longitud uno, el número anterior se reducía en un factor de 0,4 cada vez que aparecía uno de estos ciclos. Por tanto, como $105456 \cdot 0{,}4^{12} = 1{,}7$ es muy posible que doce o trece *females* determinen de manera unívoca el orden de los rotores y el *Ringstellung*.

Usando la teoría de probabilidades se deduce que, si las permutaciones Π_i y el *Grundstellung* se eligen aleatoriamente, el $11,5\,\%$ de las cabeceras presentarán *females*. Esto implica que se requiere de poco más de un centenar de mensajes para obtener una docena de ellas, cantidad factible de ser alcanzada en algunas de las redes de comunicaciones del Ejército alemán. Por tanto, es posible determinar el orden de los rotores y el *Ringstellung* a partir de las *females*.

En consecuencia, ahora sería necesario crear un catálogo de *females* para los 17576 productos posibles y compararlos con las *females* presentes en las claves del mensaje durante un determinado día.

4.2. Métodos criptológicos

La dificultad de la anterior tarea radica en la realización de las comparaciones. Esta labor, a menos que se disponga de tecnología, engloba muchas dificultades. Sin embargo, a Zygalski se le ocurrió un ingenioso método para llevarla a cabo.

Hojas de Zygalski

El método de las *hojas de Zygalski*, basado en la repetición de *females*, resultó ser bastante efectivo, aunque rudimentario. Para cada uno de los órdenes posibles de los rotores y para cada una de las posiciones del rotor izquierdo, se confeccionaron unas hojas como las que podemos ver en la Figura 4.3. Dichas hojas, de material bastante grueso, se clasificaron en paquetes, donde cada uno de ellos representaba una posible configuración de los rotores. Por tanto, hizo falta construir $6 \times 26 = 156$ hojas.

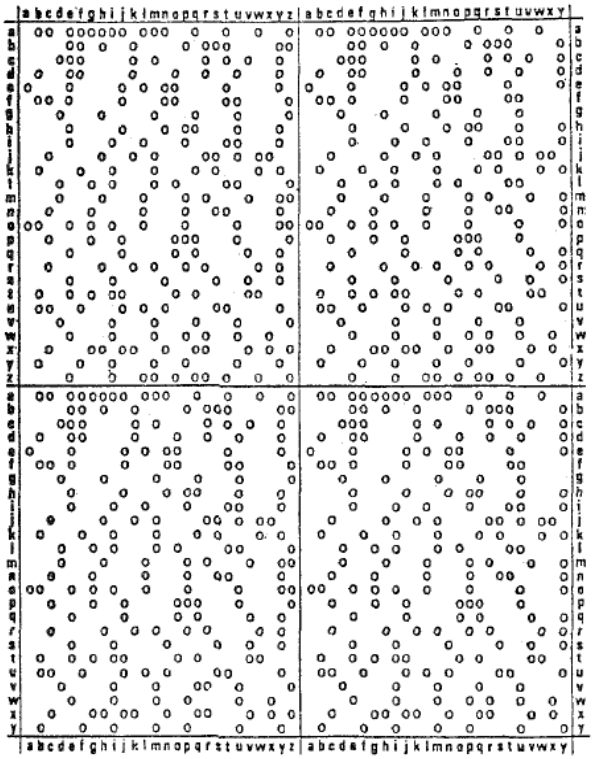


Figura 4.3: Hoja de Zygalski.

En cada una de las hojas se dibujó un peculiar sistema de coordenadas en el que los ejes marcaban las sucesivas posibles posiciones de los rotores central y derecho. Así, tanto en las abcisas como en las ordenadas se rotularon todas las letras del alfabeto, comenzando por la esquina superior izquierda. Las letras horizontales representaban las posiciones del rotor central y las verticales las del derecho.

Este sistema de coordenadas, que delimitaba un recuadro en la hoja, se dividió en 51×51 cuadrados pequeños. Cada uno de ellos representaba una permutación para esa determinada posición de los rotores. Si en dicha posición se hallaba una $1,4-$*female*[11], el recuadro correspondiente sería perforado.

[11]Recordemos que las hojas se construyeron en base a las posiciones del rotor izquierdo.

Antes de emplear las hojas es preciso realizar un proceso de "normalización" a las 2,5− y 3,6−*females*. Este proceso consiste en adelantar una posición el *Grundstellung* de las 2,5−*female* y dos posiciones el de las 3,6−*female*.

Ejemplo. Usando el ejemplo de la sección 4.1.2, la normalización consistiría en lo siguiente:

```
DQY DWJMWR    ⟹    DRY DWJMWR
HPN RAWKTW    ⟹    HPP RAWKTW
```

Realizada la normalización, el siguiente paso a realizar sería repetir el proceso anterior para cada orden de los rotores y cada posición del *Ringstellung* correspondiente al rotor izquierdo. A continuación, una vez fijado el orden de los rotores, se procede a normalizar de nuevo aquellas *females* cuyo *Grundstellung* indique un avance del rotor central.

Ejemplo. Supongamos lo siguiente:

- El orden de los rotores es `III I II`.
- El *Grundstellung* es `REJ`.

Dicho *Grundstellung* debe ser normalizado a `RFJ`, ya que la `J` es la letra que provoca en el rotor `III` un avance del rotor situado inmediatamente a su izquierda, en este caso el rotor central, donde se encuentra el `I`.

Seguidamente, se seleccionan las 26 hojas asociadas al orden de los rotores establecido y se aparta el resto. Ahora, fijada una letra del *Ringstellung* del rotor izquierdo, se considera el *Grundstellung* de una primera *female*.

Ejemplo. Consideramos lo siguiente:

- Fijamos la letra `R` en el *Ringstellung* del rotor izquierdo.
- Tenemos, entre otras, las 1,4−*females* `TUR` y `ZYG`.

Tenemos que `T - R = C`, por lo tanto, usaremos la letra `C` como patrón básico sobre el que comenzar a trabajar.
Escogemos la hoja correspondiente a dicha letra y la colocamos encima de una mesa transparente iluminada por debajo. Seguidamente, tomamos la otra 1,4−*female*: `ZYG`. Como `Z - R = I`, seleccionamos la hoja correspondiente a `I` y la colocamos sobre el patrón básico representado por la letra `C`, desplazándola 22 cuadros hacia la derecha[12] y 11 cuadros hacia abajo[13].

Una vez realizado el proceso descrito en el ejemplo anterior, repetimos la operación con el resto de *females*. Tras colocar todas las hojas, se hace actuar

[12] De la `Y` a la `U` van 22 letras.
[13] De la `G` a la `R` van 11 letras.

un foco de luz sobre ellas y se observa si la luz traspasa algún agujero común a todas ellas. Si se consigue una cantidad suficiente de *females*, el haz de luz atravesará un único agujero. Dicho agujero proporcionará de manera inmediata el orden de los rotores y el *Ringstellung* del rotor izquierdo.

Llegados a este punto, el trabajo se centraría en conseguir el *Ringstellung* de los otros dos rotores. Para ello, se observó que, fijada una de las *females* (normalizada previamente si era necesario), las letras del agujero de la hoja correspondiente determinaban la posición de los rotores que habían producido dicha *female*. Dicha posición era precisamente la diferencia entre el *Grundstellung* de la *female* y el *Ringstellung* que se pretendía obtener, ergo para obtener el *Ringstellung* de los rotores central y derecho bastaba con restar al *Grundstellung* de una *female* las letras del agujero.

El trabajo anteriormente expuesto, aparte de consumir muchísimo tiempo, resultó ser bastante tedioso, ya que, entre otras cosas, cada *female* debía ser perforada hasta cuatro veces. Sin embargo, los criptoanalistas tuvieron una observación que reduciría en gran medida dicho trabajo. Esta observación se recoge en el siguiente comentario realizado por Rejewski[14]:

"*Cuando las hojas de papel estaban situadas una sobre la otra de acuerdo a un programa precisamente definido, en el orden adecuado y desplazadas propiamente una respecto a la otra, el número de perforaciones disminuía gradualmente. Si disponíamos de un número adecuado de claves con ciclos de longitud uno, al final una misma perforación aparecería en todas las hojas de papel, probablemente correspondiendo a un buen caso*".

Así, se puede deducir que, teniendo un cantidad suficiente de datos, finalmente obtendríamos la solución.

Además, a partir de la posición de la perforación mencionada en el comentario, se podría calcular el orden de los rotores y la disposición de sus anillos. Y, comparando las letras del cifrado de la clave con las letras de la máquina, podríamos deducir, de la misma forma, la permutación S. En otras palabras, obtendríamos la clave completa del cifrado.

Finalmente, faltaría obtener las conexiones del *Stecker*. Recordemos que este no cambiaba la estructura de los ciclos, sino que únicamente alteraba las letras de los mismos. Por consiguiente, en este caso, el *Stecker* cambiaba las letras de los ciclos de longitud uno del catálogo de características por las letras repetidas de las *females*. Así, la letra repetida de una *female* estaría conectada con una de las letras de los ciclos de longitud uno de la correspondiente permutación $\Pi_4 \cdot \Pi_1$ del catálogo. De este modo, contemplando todas las *females* al mismo tiempo, no sería difícil averiguar de qué letra se trataba.

[14]Extraído de: [5].

Además de la dificultad del trabajo tenemos que considerar una dificultad añadida. Se podría dar el caso de que el haz de luz atravesase más de un agujero. Si este hecho se daba, se procedía a realizar las anteriores operaciones con cada uno de ellos, y las contradicciones descartarían casi todos los casos. Si, aún así, seguimos teniendo más de uno, elegiríamos como solución correcta aquella que permitiese descifrar los mensajes.

De forma adicional al trabajo realizado por Zygalski, Ròżycki diseñó un método para identificar el rotor derecho.

Método del reloj

El *método del reloj* desarrollado por Jerzy Ròżycki hacía posible determinar, en ocasiones, cuál de los rotores ocupaba la posición del rotor derecho[15], basándose fundamentalmente en las características propias del lenguaje alemán, es decir, en la frecuencia de aparición de las letras de su alfabeto. Veamos un ejemplo para observar en qué consistía dicho método.

Ejemplo. Supongamos que tenemos los siguientes textos[16] en alemán:

B E G I N N D E S U N E I N G E S C H R Ä N K T E N ...
S I E W E R D E N D E N P R Ä S I D E N T E N S O G ...

Observando las letras marcadas, podemos deducir que de media existirá una probabilidad de coincidencia de letras en ambos textos de 2/26. 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[17], resultaría:

N W T D T Y B X Y F T T A A A R J E P J P E U P O Y ...
S I E W E R D E N D E N P R A S I D E N T E N S O G ...

En este caso aparecen 3 letras marcadas, por lo que de media la probabilidad de coincidencia será 3/26.

El hecho de la diferencia de probabilidad entre el texto en claro y el cifrado se debe a la distinta frecuencia de aparición de las letras en idioma alemán. En un lapso de 26 letras este hecho no ocurrirá demasiadas veces. Si por el contrario se dispusiera de dos mensajes de 260 letras, con este método se podría diferenciar, normalmente, si dos mensajes habían sido cifrados con la misma clave o con diferente. Por tanto, si se disponía de una cantidad suficiente

[15] Este método cobró vital importancia en el momento en el que los alemanes decidieron comenzar a cambiar el orden de los rotores cada día.

[16] Corresponden al telegrama Zimmermann. Extraído de [11].

[17] Han sido encriptados, mediante el simulador, con las claves `TUR` y `REJ` y las conexiones `AT DS IJ MO WZ XY` del *Stecker*.

de material cifrado, en general, se podría encontrar una docena de pares de mensajes tales que en cada pareja las primeras dos letras de las claves eran idénticas y las terceras diferentes. Entonces se procedía a escribir el mensaje uno encima del otro.

Existían dos formas de escribir los mensajes uno sobre el otro, dependiendo de la posición que ocupara el rotor derecho tras producirse el desplazamiento del central. Dichas posiciones eran conocidas y diferentes para cada uno de los rotores.

Ejemplo. Supongamos que tenemos las *Spruchschlüssels* `TFG` y `TFP`, las cuales coindicen en sus dos primeras letras. Diferenciemos casos para ver lo que ocurriría para cada posición del rotor derecho.

1. El rotor de la derecha es el `I`. El rotor `I` hace avanzar al de su derecha en el momento en el que la `T` de su anillo se hace visible en la ventanilla del rotor. Entonces de `TFT` se pasa a `TFU`. Por tanto, partiendo de `TFG` nunca se llega a `TFP`.

2. El rotor de la derecha es el `II`. Análogo al anterior, ya que de `TFG` se pasaría a `TGH`.

3. El rotor de la derecha es el `III`. En este caso de `TFG` se llega a `TFP` al cabo de 9 pasos. Ya que para que se produzca el avance del rotor vecino, el rotor derecho debe llegar hasta la posición `O`. Por tanto, en este caso:

   a) La décima letra del mensaje que arranca con `TFG` se cifra con la misma permutación que la primera letra del mensaje que parte con `TFP`.

   b) Análogamente, la undécima se cifrará con la misma que la segunda.

   c) Lo mismo ocurriría con el resto.

Por tanto, colocando los criptogramas uno debajo del otro y desplazando el segundo 9 lugares[18], el número de letras coincidentes será el mismo que el de los textos en claro.

En el idioma alemán el porcentaje de coincidencias es de 7,6. Luego, si el porcentaje de coincidencias se aproxima a ese número, muy probablemente estemos en el caso en el que el rotor derecho es el `III`. Si, en cambio, el porcentaje ni se acerca a ese valor, el rotor derecho será el `I` o el `II`. En ese caso, probaríamos el mismo procedimiento con otro par de *Spruchschlüssels* con las dos primeras letras iguales.

Para cubrir la necesidad de calcular las posiciones de los rotores central y derecho a partir del *método del reloj*, se desarrolló otro, el denominado *método* ***ANX***.

[18]Para que su primera letra quede debajo de la décima del primero.

Método ANX

El *método* ***ANX*** surgió a partir de la observación de los mensajes en claro de los que disponían los polacos. Recordemos que dichos mensajes fueron descifrados gracias a las *Tageschlüssels* proporcionadas por *Asché*. Los criptoanalistas descubrieron que el texto en claro de muchos mensajes alemanes empezaba por `ANX`[19]. Por tanto, una vez determinada la posición del rotor derecho en un mensaje que comience con ese trigrama, la de los otros dos rotores se puede obtener mediante la utilización del *catálogo de características*.

Además de los métodos anteriormente descritos para la reconstrucción de las claves, fueron usados otros dispositivos mecanizados para cubrir la necesidad que iba surgiendo en distintas ocasiones. Entre ellos se encuentra la *bomba criptológica*, la última aportación de Rejewski.

4.3. Bomba criptológica

El método de la "bomba criptológica"[20] consiste mayormente en la automatización y aceleración del proceso de reconstrucción de las claves diarias. Su apariencia física la podemos ver en la Figura 4.4[21].

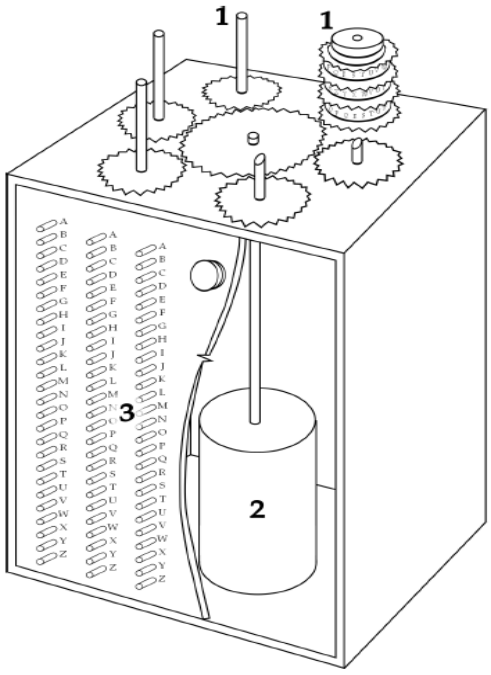


Figura 4.4: Bomba criptológica.

[19]En alemán *AN* significa para y la *X* era usada para separar palabras.

[20]Se dice que a Rejewski se le ocurrió la idea de este método mientras comía un típico helado en forma de esfera llamado bomba, de ahí ese nombre.

[21]1. Rotores; 2. Motor eléctrico; 3. Interruptores.

Esencialmente, la bomba de Rejewski es un aparato electro-mecánico basado en la combinación de tres ciclómetros conectados convenientemente y un motor eléctrico que hace girar de forma sincronizada los seis bancos de rotores recorriendo las 17576 posibles posiciones. Dado que los rotores podían ser colocados de seis formas diferentes, fue necesario construir seis bombas, una para cada orden.

De esta forma, con cada mensaje interceptado, se desarrollaba una *tabla de relaciones* (como la que aparece en el cuadro 3.1) para encontrar las cadenas resultantes, y con estas se acudía al catálogo, encontrando, así, la disposición de los rotores de la clave del día. Por tanto, el único problema restante era el de conocer las conexiones del *Stecker*.

Para resolver el problema del clavijero, Rejewski actuó de la siguiente forma: una vez conocida la disposición de los rotores, quitaba todos los cables y comenzaba a teclear el texto del mensaje. Frecuentemente el resultado obtenido era un galimatías, puesto que se desconocía las conexiones del clavijero. Sin embargo, cuando se conseguían textos muy parecidos a algo razonable, se deducía fácilmente qué letras estaban intercambiadas. Así, con una cantidad suficiente de material cifrado, era posible deducir todas las posiciones del clavijero.

Ejemplo. Supongamos que obtenemos el mensaje `INVADIT PELENIA`. De aquí se deduce fácilmente que el mensaje original sería `INVADIR POLONIA`. Por lo tanto, en este caso, se veía claramente que `R` y `T` habían sido intercambiadas, así como `O` y `E`.

Previamente a la utilización de estos aparatos, era necesario ajustar adecuadamente las posiciones de los rotores correspondientes a los ciclómetros. Para ello, primero se debería normalizar las *females* a través del método explicado en la sección 4.2.1. Hecho esto, 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 conjunto desplazado tres posiciones respecto a su correspondiente del primer conjunto. Veamos el procedimiento que seguía la bomba mediante el siguiente ejemplo.

Ejemplo. Supongamos que disponemos de tres *females* para un día determinado en las que se presentan las mismas letras repetidas[22].

```
RTJ WAHWIK
DQY DWJMWR
HPN RAWKTW
```

La primera de estas *females* indica que el ciclo `W` está presente en la permutación $\Pi_4 \cdot \Pi_1$. Supongamos que la `W` no se ve alterada por el *Stecker*, es decir,

[22]Tomamos las mismas que usamos en el ejemplo de la sección 4.1.2.

que no está intercambiada con ninguna otra letra. Entonces, también el ciclo `W` aparece en la permutación $\Pi_4 \cdot \Pi_1$ que se obtendría sin ninguna conexión del *Stecker*. Como ya sabemos, el número de tales productos $\Pi_4 \cdot \Pi_1$ es 105456, tantos como configuraciones posibles de los rotores (orden y posiciones iniciales). Ahora bien, desconocemos cuántos de estos productos contienen al ciclo `W`. No obstante, recordemos que la teoría de probabilidades muestra que, fijado un ciclo de longitud 1, si Π_1 y Π_4 se eligen aleatoriamente entre las de su clase, entonces el 4 % de los productos $\Pi_4 \cdot \Pi_1$ contienen dicho ciclo. Admitamos esta regla para las sustituciones de Enigma. Entonces, el anterior número se reduce en un factor de 0,04 cada vez que se observe una *female* con la letra `W` repetida. Como $105456 \cdot 0{,}04^3 = 6{,}75$, resulta que muy probablemente tan solo seis o siete configuraciones de los rotores pueden ocasionar las tres *females* anteriores.

El objetivo de la bomba era, por tanto, automatizar la identificación de las configuraciones de las que hablábamos en el ejemplo del siguiente modo: en el momento en el que los tres ciclómetros que componen la bomba reconocen el ciclo `W`, el mecanismo se detiene mostrando posición.

En nuestro ejemplo, los rotores del ciclómetro asociado a la primera *female* deben colocarse del siguiente modo: el primer conjunto en la posición `RTJ` y el segundo en la `RTN`. Tras situar los rotores se activa la palanca de la letra `W` y se pone en marcha la bomba. Las seis bombas encontrarían las seis o siete posiciones posibles que ocasionaban las tres *females* y, entre ellas, se hallaría la que proporcionaba la clave. Para poder conocerla era necesario aplicar el método de las *hojas de Zygalski*.

Este método, aunque provocó que una gran cantidad de personas se dedicaran a él, congregando a alrededor de 100 trabajadores, hizo que se acortara el tiempo para la obtención de la clave a aproximadamente dos horas.

Cuando parecía que los polacos ya habían logrado descifrar la máquina y que no les supondría ningún impedimento desencriptar los mensajes que los alemanes se enviaban, surgieron nuevos problemas. Los alemanes introdujeron dos rotores más, incrementaron las conexiones del clavijero de seis a trece pares y el número de redes de comunicaciones de radio alemanas también creció. Debido a todo ello, los métodos anteriormente descritos quedaron inservibles, ya fuese por la falta de presupuesto, personal o la inoperancia de estos.

Para más añadidura, tal y como mencionábamos en el capítulo 1, Polonia llegó a encontrarse duramente amenazada por los alemanes. Este cúmulo de acontecimientos provocó la búsqueda de aliados (franceses y británicos) que pudieran aprovechar los trabajos realizados por los polacos.

Índice de figuras

Apéndice A

Referencias de figuras

- Patente americana de Enigma: [8].

- Diagrama de las partes de Enigma: [8].

- Rotores de Enigma: *Collingwood reunites crucial dials with German code machine they once powered.* https://navynews.co.uk/archive/news/item/4671 (Navy News, Royal Navy UK).

- Circuito eléctrico de Enigma: [4].

- Diagrama de funcionamiento de Enigma: [8].

- Recorrido de la corriente eléctrica a través de Enigma: [6].

- Ciclómetro: [6].

- Diagrama del ciclómetro: [6].

- *Hoja de Zygalski*: [6].

- *Bomba criptológica*: [6].

Apéndice B

Referencias por capítulos

A continuación se presentan las referencias mayormente usadas en cada capítulo, sin referencia explícita.

- Capítulo 1: [3], [1], [8].
- Capítulo 2: [8], [4], [10].
- Capítulo 3: [7], [8], [4], [9].
- Capítulo 4: [8], [4], [6], [5].

Referencias generales

[1] Ceano, R.: *La máquina Enigma*. http://www.kryptopolis.com/enigma

[2] Christensen, C.: *Polish mathematicians finding patterns in Enigma machine*. Mathematics Magazine **80** (2007) 247–273.

[3] Fernández, S.: *La criptografía clásica*. Revista SIGMA **24** (2004) 119–141.

[4] García del Castillo Crespo, E.; López, M.A.; Ortega Triguero, J.J.: *Introducción a la Criptografía. Historia y actualidad*. Servicio de Publicaciones de la Universidad de Castilla–La Mancha (2006).

[5] Rejewski, M.: *How Polish mathematicians deciphered the Enigma*. Annals of the History of Computing **3** (1981) 213–234.

[6] Rejewski, M.: *Mathematical solution of the Enigma cipher*. Cryptologia **6** (1982) 1–18.

[7] Rotman, J.J.: *An introduction to the theory of groups*. Springer (1999).

[8] Sánchez Muñoz, J.M.: *Historias de Matemáticas. Criptología Nazi. Los códigos Secretos de Hitler*. Pensamiento Matemático **III** (2012) 59–120.

[9] Smart, N.P.: *Cryptography: An Introduction*. (online 2nd edition). McGraw–Hill (2002).

[10] Soto, M.J.; Tornero, J.M.: *Notas de Teoría de Códigos y Criptografía*. Departamento de Álgebra, Universidad de Sevilla (2015).

[11] https://de.wikipedia.org/wiki/Zimmerman-Depesche

[12] http://www.amenigma.com

[13] http://enigmaco.de/enigma/enigma.swf