El uso de permutaciones para encontrar el cableado de la máquina Enigma

Sandra Paño Badía
Trabajo de fin de grado en Matemáticas
Universidad de Zaragoza

Directora del trabajo: Paz Jiménez-Seral
27 de junio de 2017

Summary

In September 1932, Marian Rejewski was hired by Polish Cipher Bureau to decrypt encrypted messages with the Enigma machine, a machine used by the German army to encrypt internal communications and then used during World War II. Rejewski, Jerzy Rozycki and Henryk Zygalski were the first mathematicians hired by a government to work on cryptography. Until that moment, this work has been done by linguists. Since then, cryptology has been done by mathematicians and computer scientists.

The Enigma machine is an half-electric, half-mechanical device. The mechanical part consists on a keyboard as the one used by typewriters, a panel with lamps and a mechanical inside, composed of a series of rotors and connections. The electrical part has an electric circuit which is closed by pressing one of the keys in the keyboard and this circuit lights up the lamp which corresponds with its encrypted letter.

First of all, Rejewski only had a commercial Enigma machine, with its instruction book and hundreds messages intercepted to the Germans.

By using only the hundreds messages intercepted as facts, Rejewski realized that the first six letters of a message came from a three-letter repetition (he learned that they were used as the key of the message later). Using these first six letters in the messages intercepted and his knowledge of the theory of the permutations, he managed to find the first six permutations generated by Enigma, that is how the first six letters that were entered in the machine were encrypted. Once he obtained these permutations, it was easy to find the keys of the message that the corresponding soldier has sent. In addition, by finding these keys, clues were obtained about the keys used other day by the same soldier. Obtaining these first six permutations was a simple process, so they could be obtained from any day.

Looking at the machine and using his knowledge of permutation?s theory, Rejewski deduces the equation that models the working of the machine:

$$\boxed{\alpha = \sigma\pi^{c+1}\nu\pi^{-c-1+b}\mu\pi^{-b+a}\lambda\pi^{-a}\rho\pi^{a}\lambda^{-1}\pi^{b-a}\mu^{-1}\pi^{c+1-b}\nu^{-1}\pi^{-c-1}\sigma}$$

This equation corresponds to a given order of the rotors, I-IV-V, at a concrete given time.

Each of the permutations in this formula refers to each parts of the machine:

Rotor I	Rotor IV	Rotor V	Plugboard	Reflector
λ	μ	ν	σ	ρ

And π is the permutation that carries each letter to its next in alphabetical order.

Since $\rho = \rho^{-1}$ and α is a conjugate permutation of ρ, also $\alpha = \alpha^{-1}$. This justifies that using exactly the same machine configuration we can encrypt and decrypt messages. The sodier who sent the message and recipient soldier set the machine in the same way.

After a while, Rejewski got a notebook of keys, with keys of two different months. In these notebooks, the keys, which were necessary to configure Enigma, were pointed out, in order to be able to encrypt and decrypt.

These keys were given as follows, for example:

Rotor Order	Rotor settings	Absolute Position	Plugboard
I-IV-V	SPB TFG	(1, 16, 5)	(e n)(i g)(m a)(r w)(s k)(p b)

There are point out the used rotors (three of a possible five are used) and their order, the ring setting and the window setting of the rotors, the joint adjustment of the rotors (it is deduced from the rotor adjustments) and the connections of the plugboard. It was not necessary to indicate the reflector used because there was only one, later another one was introduced.

Using the equation that models the running of the machine and one of the days of the codebook, Rejewski was able to deduce the wiring except for twist from the rotor to the right of the machine. With this method, it is only possible to obtain the wiring except for twist of two rotors, since he only had the keys of two months (in each one the right rotor was different, one with I-IV-V rotors order and another with I-V-IV). Thus two permutations, μ_0 and ν_0 are obtained, for example, showing rotor wiring except for twist.

$$\nu_0 = (a)(b\ e\ l\ i\ z\ p\ c\ g\ y\ h\ d\ w\ k\ x\ j\ u\ v\ t\ o\ q\ f\ n\ m\ s\ r)$$

$$\mu_0 = (a)(b\ o\ t\ c\ k\ q\ j\ m\ n\ d\ r)(e\ l)(f\ v\ z\ x\ i\ u\ g)(h\ w\ y\ s\ p)$$

Rejewski in his works [3] [4] stated that once the wiring of these rotors is found find the twisting, the wiring of the remaining rotor and the reflector does not present great difficulties, but he does not explain how it would be done. He also adds that obtaining rotor turnover was not difficult to determine but still fails to explain how he achieved it. From this point, the procedure described in [5] is followed with different data.

The wiring of each of these two rotors, taking into account the twisting, is given by:

$$\nu = \nu_0\pi^n, n \in 0,...,26$$

$$\mu = \mu_0\pi^m, m \in 0,...,26$$

To end finding the wiring of these two rotors it is necessary to find the twist, that is, to find the exact values of m and n in this case. To do this, it is used the equation that models the machine. Using two different days of the keybook and the two equations that model the machine in those two days, we obtain the values of n and m, 21 and 4 respectively. And so, get the wiring of the two rotors:

$$\boxed{\nu = \nu_0\pi^{21} = (a\ v\ o\ l\ d\ r\ w\ f\ i\ u\ q)(b\ z\ k\ s\ m\ n\ h\ y\ c)(e\ g\ t\ j\ p\ x)}$$

$$\boxed{\mu = \mu_0\pi^4 = (a\ e\ p\ l\ i\ y\ w\ c\ o\ x\ m\ r\ f\ z\ b\ s\ t\ g\ j\ q\ n\ h)(d\ v)(k\ u)}$$

Once the wiring of two of the rotors is obtained, it proceed with the calculation of the remaining rotor wiring (located to the left in any of the two months we have). For this calculation, apart from being necessary the equation which reflects the operation of Enigma, it is necessary to use the data from four different days. Adapting the equation with data already obtained and taking into account unknowns, we obtain the wiring of the remaining rotor except for the twist:

$$\lambda_0 = (a)(b\ g\ z\ f\ c\ i\ r\ q\ t\ l\ p\ d)(e\ h\ m\ k\ j\ v)(n\ s\ o\ u\ w\ x)(y)$$

Before proceed with the calculation of the twist of this rotor, it is necessary to find the wiring of the reflector up to conjugation. The procedure is similar to the one used to find the wiring except twisting of last rotor. It is necessary the keys of a day and adapt the equation of the model with the known data, it changes with the previous one because λ_0 is now known.

Thus, we obtain that the wiring up to conjugation of the reflector is::

$$\rho_0 = (r\ x)(t\ i)(h\ v)(o\ q)(g\ n)(f\ z)(k\ c)(a\ e)(s\ j)(d\ u)(w\ b)(y\ l)(m\ p)$$

It is necessary to find the corresponding twist, that is, to find l in order to obtain the wiring of last rotor and the reflector.

$$\lambda = \lambda_0\pi^l, l \in 0,...,26$$

$$\rho = \pi^{-l}\rho_0\pi^l$$

It is impossible to find l using data with only two different positions of the rotors.

To do this, it is necessary to use the example, which has an order of rotors V-IV-I, it belongs to the instruction manual of the machine. This example consists of a plain text, its corresponding ciphertext and the configuration used by the machine to encrypt, using this example and the equation with all the data obtained, we find that $l = 4$.

Thus, we have the wiring of the remaining rotor and the reflector:

$$\boxed{\lambda = \lambda_0 \pi^4 = (a\ e\ l\ t\ p\ h\ q\ x\ r\ u)(b\ k\ n\ w)(c\ m\ o\ y)(d\ f\ g)(i\ v)(j\ z)(s)}$$

$$\boxed{\rho = \pi^{-4} \rho_0 \pi^4 = (a\ f)(b\ v)(c\ p)(d\ j)(e\ i)(g\ o)(h\ y)(k\ r)(l\ z)(m\ x)(n\ w)(q\ t)(s\ u)}$$

At last, seeing how the rotors of the Enigma machine works it is necessary obtain the turnover of these. Turnover is an effect that occurs in the machine when a certain letter appears in the window of one of the rotors, then a notch that has the rotor causes the rotor to the left turns $\frac{1}{26}$ revolution.

To find the turnover of the rotor I, the example given in the instruction book is used. It is a matter of checking that by applying the equation modeling Enigma to the letter in the i-th position of the plaintext results in the letter in the i-th position of the ciphertext. So until it reflects a contradiction..

$$\boxed{The\ turnover\ of\ the\ rotor\ I\ is\ the\ letter\ Q}$$

Finally, in order to find the letter of the turnover in the remaining two rotors, we use the equation governing the operation of Enigma. We use one of many messages intercepted to Germans on one of the days in the keybook. Let's decipher that message with the formula until the time in which the plain text does not make sense.

$$\boxed{The\ turnover\ of\ the\ rotor\ IV\ is\ the\ letter\ J}$$

$$\boxed{The\ turnover\ of\ the\ rotor\ V\ is\ the\ letter\ Z}$$

Índice general

Capítulo 1

Introducción

1.1. Introducción Historica

En tiempos de guerra, el comunicarse con los aliados sin que los enemigos obtuvieran la información sobre la próxima ofensiva ó la disposición de las defensas era de vital importancia. Por lo tanto era importante el poder comunicarse de forma que los enemigos no entendieran los mensajes enviados. La criptología es el método usado para poder enviar toda esta información de forma secreta.

En la Primera Guerra Mundial fue decisivo el descifrado de un mensaje enviado por el ministro de asuntos exteriores alemán, Arthur Zimmerman [1]. Este mensaje fue interceptado por los ingleses los cuáles se lo mostraron a los americanos y por ello tomaron parte en la guerra. Fueron usados muchos métodos de cifrado pero todos eran más ó menos versiones modificadas de métodos antiguos. Unos de los métodos que se modificaron y fueron muy usados eran la rejilla de Cardano y el cifrado de Polibio. De este último surgió el llamado cifrado ADFGX.

Después de los fracasos obtenidos durante el envío de mensajes secretos en la Primera Guerra Mundial, los alemanes se dieron cuenta de que era necesario desarrollar nuevos métodos de cifrado para poder asegurar la seguridad de sus comunicaciones. Este fue el trabajo del ingeniero electrónico alemán Arthur Scherbius. Arthur creó una máquina criptográfica electromecánica llamada Enigma.

La fama de esta máquina llegó hasta España, Franco de hecho uso un modelo de Enigma durante la Guerra Civil. Después de la guerra, el régimen siguió usandola hasta los años 50. [1]

Polonia fue el primero gobierno en contratar matemáticos para trabajos de criptágrafos, hasta entonces este trabajo lo densempeñaban lingüistas. En 1932, Polonia contratató a tres matemáticos con el propósito de descifrar Enigma, Marian Rejewski, Jerzy Rozycki y Henryk Zygalski [1] [4]. Desde entonces toda la criptología está en manos de matemáticos e informáticos. En Octubre de 1932, Rejewski y sus compañeros disponían de los siguientes documentos para el descifrado de la máquina:

• Una colección de mensajes cifrados con Enigma, los cuales fueron interceptados por el servicio de inteligencia polaco. Cada día interceptaban mensajes nuevos.

• Las instrucciones de Enigma, datado en 1930, el cuál contenía un ejemplo completo, esto es un texto sin cifrar y su correspondiente cifrado con Enigma y la clave utilizada. Material suministrado por el servicio de inteligencia francés.

• Una lista de claves de cada día de Septiembre y Octubre de 1932. Material suministrado por el servicio de inteligencia francés.

• Una versión comercial de Enigma. Este modelo difiere del usado por los alemanes en que el modelo militar posee clavijero y que las conexiones del teclado cambian. También difiere el sistema de turnover. Los rotores y el reflector de cada modelo poseen diferente cableado interno.

Rejewski y sus colegas consiguieron construir una réplica más ó menos precisa del modelo militar. Aun así esto resultó insuficiente, ya que cumplía uno de los principales principios de criptografía, el Principio de Kerckhoffs, el cuál asegura que la fortaleza de un sistema de cifrado reside en la clave empleada en el proceso y no en el método de cifrado. Por lo tanto, en el caso de Enigma debía mantenerse en absoluto secreto las claves utilizadas para cifrar. Pero las posibles claves ascendían a miles de

millones. Incluso con las herramientas matemáticas que desarrollaron el proceso de desencriptación era largo y tedioso, por ello los polacos construyeron máquinas, llamadas bombas, para agilizar el proceso.

Pero esta alegría duro poco. Los alemanes introdujeron varias modificaciones en Enigma: los tres rotores ahora eran cinco, intercambiables además, y el clavijero se amplió. [4]

El 1 de Septiembre de 1939, Alemania invadía Polonia. Dos días después, Francia e Inglaterra le declaraban la guerra a Alemania y así comenzó la Segunda Guerra Mundial.

Antes de ser invadidos, los polacos enviaron toda la información recopilada sobre Enigma a los servicios de inteligencia franceses e ingleses. Los ingleses siguieron estudiando Engima y desencriptaron mensajes con nuevas bombas.

1.2. Aspecto y Ajustes

La máquina Enigma es un aparato medio eléctronico, medio mecánico. Consta de las siguientes partes:

• Un teclado con las 26 letras del abecedario.

• Un panel con las 26 letras con una lámpara debajo de cada letra.

• Una parte donde se colocan los rotores. En todo el trabajo se va a referir a una máquina con tres rotores que se eligen entre cinco posibles. Los tres rotores se colocan en la máquina en un mismo eje perpendicular. Cada rotor tiene asociada una ventanilla mostrando una letra. En su interior, cada rotor dispone de un anillo con las 26 letras del abecedario y una muesca. Además poseen un circuito interno con 26 puntos de entrada y el mismo número de puntos de salida, uno por cada letra. Es importante comentar que cada rotor tiene dentro una muesca la que hace que se produzca un efecto llamado turnover, dicho efecto lo que hace es que cuando una determinada letra aparece en la ventanilla la muesca hace que el rotor contiguo a la izquierda gire $\frac{1}{26}$ de vuelta. Cada rotor tiene su propia letra asociada a dicha muesca, se llama turnover letter.

• Situado en el mismo eje de los rotores se encuentra un disco llamado reflector. Hay dos posibles reflectores a elegir.

• Por último, consta de un clavijero con un orificio por cada una de las letras. Dispone de conectores (cables) para conectar orificios correspondientes a letras emparejadas dos a dos. En este caso, el clavijero consta de 6 conectores.

Para configurar la máquina adecuadamente se necesita conocer unas claves. Esta clave para la configuración consta de varios elementos. Algunos de ellos no varían en meses, otros en días y otros cambian en cada mensaje. La configuración de Engima esta formada por lo siguientes elementos:

• Los rotores utilizados y su disposición. Qué rotores de los cinco posibles se deben elegir y en que posición se colocan. Por ejemplo: III-II-I.

• El reflector utilizado. Hasta más adelante no se introdujo un segundo reflector a elegir.

• Ajuste interno de los rotores (ring setting). Se trata de tres letras las cuáles se tienen que ajustar en una muesca disponible en cada uno de los anillos que poseen los rotores. Es decir, si tenemos como ajuste interno UNI tenemos que tomar el rotor III (todo este ajuste se realiza de acuerdo al orden y selección de los rotores) y ajustamos en anillo interno de manera que la U encaje en la muesca nombrada. De manera análoga procederíamos con los otros dos rotores.

• Encajar el reflector y los rotores en el orden indicado.

• Ajuste externo de los rotores (window setting). Se trata de otra terna de letras. Una vez colocados los rotores en la máquina, estos se ajustan manualmente, haciendolos girar, hasta que la letra de la terna correspondiente se ve en la ventanilla situada al lado de cada rotor. Por ejemplo: sea el ajuste externo ZAR, se gira manualmente el rotor III hasta que aparezca en la ventanilla la letra Z. De manera análoga se procede con los otros dos rotores.

• Finalmente se conectan los cables de clavijero como nos indique la clave.

Los soldados alemanes encargados de cifrar y descifrar mensajes poseían un cuaderno con claves que se debían usar cada día. En 1932, el orden de los rotores se cambiaba cada trimestre, el ajuste interno de los roteres cada mes y el clavijero y ajuste externo de los rotores cada día. Para proteger la clave, los

mensajes de un mismo día se intentaban cifrar con claves distintas, por ello, antes de cifrar el mensaje se seleccionaba una terna de letras aleatorias, llamadas clave del mensaje. Esta terna se introducía dos veces en la máquina, una vez esta se hubiera configurado de la manera adecuada, y a continuaciíon se cambiaba el ajuste externo para que aparecieran en las ventanillas dicha terna. Ahora se procedía al cifrado del mensaje.
Con exactamente la misma cofiguración, la máquina sirve tanto para encriptar como para desencriptar.

Lo importante del ajuste interno y externo es, en cada instante, la posición relativa de unos ajustes respecto a los otros. Más concretamente, la representación de ambas configuraciones conjuntamente, es decir, ambas configuraciones se pueden representar de una única forma mediente una terna de números **(a,b,c)**, llamada ajuste conjunto ó posición absoluta, con $0 \leq a,b,c \leq 25$, de tal forma que a corresponde al rotor de la izquierda, b al central y c al de la derecha. Este ajuste se obtiene de la siguiente manera: primero asignamos a cada letra del alfabeto un número, $A = 1, B = 2, C = 3, ...$, después realizamos la resta de los números resultantes del ajuste externo menos los del ajuste interno modulo 26. Por ejemplo, si tenemos ajuste interno UNI y ajuste externo ZAR, para el rotor de la derecha sería:

$$I \rightarrow 9 \; y \; R \rightarrow 18$$

$$(18-9) \; mod 26 = 9$$

Así, en este ejemplo el ajuste conjunto quedaría: (5, 13, 9). Notar que este ajuste externo también corresponde con el ajuste AAA-FNJ.

El ajuste externo también es importante por si solo, ya que como se ha comentado en este trabajo cada vez que se presiona una tecla la configuración externa del rotor de la derecha cambia y por lo tanto cambia el ajuste conjunto en su tercera componente.

Además cuando se producía el llamado turnover, comentado con anterioridad, cambiaba también el ajuste externo en la componente central, ya que es el rotor que ha girado $\frac{1}{26}$ de vuelta debido al efecto ocasionado por la muesca del rotor de la derecha. El mismo efecto ocurre con el rotor de la izquierda. El rotor central hace que gire el rotor a su izquierda, este efecto se llama double stepping.

1.3. Enigma por dentro (funionamiento)

Una vez configurada la máquina en una posición concreta, al pulsar una de las letras suceden simultáneamente dos efectos en la máquina:
• La fuerza con la que se presiona la tecla se transmite al rotor derecho, el cual gira $\frac{1}{26}$ partes de vuelta haciendo que en la ventanilla aparezca la siguiente letra. Además puede producirse el efecto turnover ya comentado. El sentido de giro de los rotores es horario.
• Por otra parte se cierra un circuito eléctrico de la máquina. La corriente fluye a lo largo de la máquina de la siguiente manera:

$$Teclado \rightarrow Clavijero \rightarrow Rotores \rightarrow Reflector \rightarrow Rotores \rightarrow Clavijero \rightarrow Lamparas$$

Como se ha dicho anteriormente, los rotores y el reflector poseen un cableado interno, cada uno con 26 puntos de entrada y 26 de salida. Al girar un rotor su cableado interno no varía pero si que cambian sus puntos de entrada y de salida. Por ello una letra pulsada dos veces consecutivas se cifra con dos letras distintas, ya que al menos uno de los rotores a girado.

Capítulo 2

Herramientas

En este capítulo se incluye la teoría de permutaciones usada como herramienta.

2.1. Teoría de permutaciones

Una permutación de un conjunto C no vacío es una aplicación biyectiva de C en sí mismo. Los elementos de C se llaman letras ó cifras, se usan ambos nombres de manera indistinta. Se indicaran mediante letras griegas minúsculas. Para este trabajo, se estan interesado en el conjunto

$$C = \{a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z\}$$

.

Para indicar la acción que realiza una permutación, α, se dice que α aplica la cifra i en la j y se indica con notación a a izquierda, es decir, $i\alpha = j$. Si $i \neq j$ se dice que α mueve i, en caso contrario se dice que α fija i.

Una permutación α se representa de la siguiente manera:

$$\begin{bmatrix} a & b & c & ... & z \\ a\alpha & b\alpha & c\alpha & ... & z\alpha \end{bmatrix}$$

Una perutación α se dice que es un ciclo de longitud r ó un r-ciclo si existen r cifras distintas y ordenadas, $c_1, c_2, ..., c_r$, de manera que α mueve cada cifra en la siguiente, la última en la primera y fija el resto de cifras, es decir, $c_i\alpha = c_{i+1}$ para $i = 1,2,...,r-1$, $c_r\alpha = c_1$ y $c\alpha = c$ para $c \neq c_i$. Un ciclo de estas características se suele indicar de la siguiente manera: $\alpha = (c_1\ c_2\ ...\ c_r)$. Es claro que un ciclo está determinado por esas cifras y por su ordenación, salvo por la ordenación cíclida, es decir, $(c_1\ c_2\ ...\ c_r) = (c_r\ c_1\ c_2\ ...\ c_{r-1})$. Se admite $r = 1$, un 1-ciclo es la aplicación identidad denotada por ι, y se admite $\iota = (c)$ para cualquier cifra c.

La composición de las permutaciones α y β se llama producto de esas permutaciones, se denotara simplemente por $\alpha\beta$. De acuerdo con la notación por la izquierda en el producto que se acaba de definir actúa primero α y después β, esto es: $i\alpha\beta = (i\alpha)\beta$.

Dos permutaciones se dicen disjuntas si no existe ninguna cifra que la muevan ambas permutaciones. Es claro que si las permutaciones α y β entonces $\alpha\beta = \beta\alpha$.

Como una permutación α es una aplicación biyectiva es claro que existe su permutación inversa, α^{-1}. Es sabido que $(\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1}$.

El orden de una permutación α al menor número natural r tal que $\alpha^r = \iota$. Es claro que el orden de un r-ciclo es r.

Una involución es una permutación α de orden 2, es decir, $\alpha \neq \iota$ y $\alpha^2 = \iota$. En este caso, $\alpha = \alpha^{-1}$.

Lema 2.1. *Toda permutación α se puede expresar como producto de ciclos disjuntos dos a dos. Esta expresión es única salvo en la ordenación de los factores, y en los 1-ciclos.*

Demostración. Para una cifra c_1 cualquiera, considerar la sucesión $c_1, c_1\alpha, c_1\alpha^2, \ldots$. Sea $r_1 \neq 0$ el menor exponente para el que existe $s < r_1$ con $c_1\alpha^{r_1} = c_1\alpha^s$. Se sigue $c_1\alpha^{r_1-s} = c_1$, por o que $s = 0$, es decir, r_1 es el menor número natural tal que $c_1\alpha^{r_1} = c_1$. Consideramos el r_1-ciclo $\gamma_1 = (c_1\ c_1\alpha\ \ldots\ c_1\alpha^{r_1-1})$. Sea ahora una cifra c_2 que no esté en γ_1, y de manera análoga formamos el ciclo $\gamma_2 = (c_2\ c_2\alpha\ \ldots\ c_2\alpha^{r_2-1})$, siendo r_2 el menor número natural tal que $c_2\alpha^{r_2} = c_2$. Por ser α inyectiva, estos ciclos son disjuntos. Procedemos de manera análoga hasta agotar las cifras de C. Fnalmente se ve que α es producto de todos los ciclos así formados, que son disjuntos dos a dos. La unicidad se sigue puesto que si la cifra c está en el r-ciclo γ entonces $\gamma = (c\ c\alpha\ \ldots\ c\alpha^{r-1})$.

Por ejemplo, la siguiente permutación de $C = \{a, b, \ldots, z\}$ se descompone en ciclos disjuntos de esta forma:

$$\begin{bmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ e & k & m & f & l & g & d & q & v & z & n & t & o & w & y & h & x & u & s & p & a & i & b & r & c & j \end{bmatrix} =$$

$$= (aeltphqxru)(bknw)(cmoy)(dfg)(iv)(jz)(s)$$

Decimos que un ciclo $\gamma \neq \iota$ forma parte de la permutación α si γ es uno de los ciclos que aparece en la expresión de α como producto de ciclos disjuntos. También diremos que un producto de ciclos disjuntos forma parte de α si cada uno de esos ciclos forma parte de α. En esos caso se escribe $\gamma \subset \alpha$.

Se llama tipo ó estructura de ciclo de una permutación a la sucesión decreciente de las longitudes de los ciclos de su expresión como producto de ciclos disjuntos, incluyendo en est sucesión tantos 1 como cifras fije dicha permutación. En el ejemplo anterior el tipo de la permutación sería: $(9,4,4,3,2,2,1)$.

Si tomamos un ciclo de longitud s, $\pi = (c_1\ c_2\ \ldots\ c_s)$, y r un número se tiene

$$c_i\pi^r = c_{i+r}$$

Se entiende que si $i + r > s$ se debe hacer una pequeña corrección consistente en hallar el resto t de dividir $i + r$ por s y poner

$$c_i\pi^r = c_{i+r} = c_t$$

.

Por ejemplo, sea el ciclo de longitud 26, $\pi = (abcd\ldots xyz)$, se tienen las siguientes potencias de π:

$$\pi^2 = (acegikmoqsuwy)(bdfhjlnprtvxz)$$

$$\pi^{13} = (an)(bo)(cp)(dq)(er)(fs)(gt)(hu)(iv)(jw)(kx)(ly)(mz)$$

Pero, cualquier potencia de π con exponente primo con 26 es un ciclo de longitud 26.

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

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

y se escribe $\alpha = \beta^\gamma$. También se dice que γ conjuga β a α. En el caso de que γ sea un producto de varias permutaciones, se escribe $\alpha = \gamma^{-1}\beta\ldots$ en lugar de $\alpha = \beta^\gamma$.

Proposición 2.2. *Se verifica:*
(a) $(\alpha\beta)^\gamma = \alpha^\gamma\beta^\gamma$
(b) $(\beta^\gamma)^{-1} = (\beta^{-1})^\gamma$
(c) $(\beta^\gamma)^\delta = \beta^{\gamma^\delta}$
(d) Si $\alpha = \beta^\gamma$, *entonces* $\alpha^{\gamma^{-1}} = \beta$
(e) $(c_1\ c_2\ \ldots\ c_r)^\gamma = (c_1\gamma\ c_2\gamma\ \ldots\ c_r\gamma)$
(f) Dos permutaciones conjugadas son del mismo tipo.
(g) Dos permutaciones del mismo tipo son conjugadas.
(h) Si α *y* β *son conjugadas, entonces el número de permutaciones que las conjugan es*

$$\#\{\gamma | \alpha = \beta^\gamma\} = r_1 r_2 \ldots r_s t_1! \ldots t_m!$$

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

Demostración. Los apartados (a), (b), (c) y (d) son simples comprobaciones. Para el apartado (e), sea c una cifra cualquiera. Si $c = c_j\gamma$ para algún j, se tiene

$$c(c_1\ c_2\ ...\ c_r)\gamma = c\gamma^{-1}(c_1\ c_2\ ...\ c_r)\gamma = c_j(c_1\ c_2\ ...\ c_r)\gamma =$$

$$c_{j+1}\gamma = c_j\gamma(c_1\gamma\ c_2\gamma\ ...\ c_r\gamma) = c(c_1\gamma\ c_2\gamma\ ...\ c_r\gamma)$$

Si fuese $c \neq c_j\gamma$ para $j = 1, ..., r$, como $c\gamma^{-1} \neq c_j$, se puede escribir

$$c(c_1\ c_2\ ...\ c_r)^{\gamma} = c\gamma^{-1}(c_1\ c_2\ ...\ c_r)\gamma = c\gamma^{-1}\gamma = c = c(c_1\gamma\ c_2\gamma\ ...\ c_r\gamma)$$

Luego se sigue el apartado(e).
El (f) se sigue directamente de (e). Para ver que se verifica (g) basta expresar las permutaciones que tienen el mismo tipo como producto de ciclos disjuntos y una debajo de la otra, alineando los ciclos de la misma longitud. Así, la permutación que aplica una cifra en la que se encuentre inmediatamente debajo en esa expresión, es una permutación que conjuga las permutaciones iniciales.
Finalmente, el número de permutaciones que conjugan las dos dadas se obtiene contando las formas esencialmente distintas de colocar una permutación debajo de la otra según se ha explicado en el párrafo anterior.

El apartado (f) de este teorema se conoce como El teorema que permitió ganar la segunda guerra mundial. Notar la importacia del apartado (e), ya que muestra una manera cómoda de calcular conjugaciones.

Los 2-ciclos se denominan trasposiciones. En este trabajo son importantes los productos de trasposiciones disjuntas y la descomposición de un permutación en producto de trasposiciones.

Proposición 2.3. *Una permutación que sea producto de trasposiciones disjuntas es una involución, es decir, su orden es 2. Recíprocamente, toda involución es un producto de trasposiciones disjuntas.*

Demostración. La primera afirmación se sigue del hecho de que el producto de permutaciones disjuntas es conmutativo y de que el orden de un ciclo coincide con su longitud. Para el recíproco, sea α una involución, por el Teorema 0.1 es

$$\alpha = \gamma_1\ ...\ \gamma_m,$$

con γ_i ciclos disjuntos dos a dos, por lo que se tiene

$$\iota = \alpha^2 = \gamma_1^2\ ...\ \gamma_m^2,$$

y por ser γ_i^2 disjuntos es $\gamma_i^2 = \iota$, es decir, γ_i son trasposiciones.

Lema 2.4. *Si γ y π son ciclos de longitud n siendo n el grado de C, y ν_0 conjuga γ a π, entonces el conjunto de permutaciones que conjugan γ a π es*

$$\sum = \{\nu | \nu = \nu_0\pi^k, 0 \leq k \leq n-1\}$$

Demostración. Por una parteaplicando el apartado (c) del Teorema 0.4, se ve fácilmente que todos los elementos de $\sum$ conjugan γ a π. Por otra parte, puesto que el tipo común de ambas permutaciones es (n) y por el apartado (h) del Teorema 0.4, se tiene que n es el número de permutaciones que conjugan γ a π. Finalmente se sigue el teorema porque $\sum$ tiene exactamente n elementos.

Teorema 2.5. *Teorema de Rejewski.*
(a) El producto de dos r-ciclos disjuntos es producto de dos involuciones, más concretamente

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

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

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

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

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

$$(...\ c_1\ c\ c_2\ ...)(...\ c_1'\ c'\ c_2'\ ...) \subset \alpha\beta$$

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

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

Demostración. (a) La igualdad es una simple comprobación. Ahora se sigue la afirmación teniendo en cuenta el Teorema 0.5.

(b) Por el Teorema 0.5, α y β son producto de mismo número de trasposiciones disjuntas, y por no tener puntos fijos todas las cifras están en esas trasposiciones, en particular el grado de las mismas debe ser par. Dada una cifra c, podemos formar una sucesión de $2r$ cifras distintas $c = c_1, c_2, ..., c_{2r}$ tales que

$$(c_1\ c_2)(c_3\ c_4)...(c_{2r-1}\ c_{2r}) \subset \alpha$$

$$(c_2\ c_3)(c_4\ c_5)...(c_{2r}\ c_1) \subset \beta$$

Nótese que r debe ser maor ó igual que 1. Teniendo en cuenta que ciclos disjuntos conmutan, al calcular el producto $\alpha\beta$, por el apartado (a), se sigue que

$$(c_1\ c_3\ c_5\ ...\ c_{2r-1})(c_{2r}\ c_{2r-2}\ ...\ c_4\ c_2) \subset \alpha\beta$$

Si con las cifras anteriores se han agotado todas las cifras, el teorema ha quedado demostrado, en caso contrario tomamos otra cifra c_{2r+1} y procedemos de forma análoga hasta agotar todas las cifras de C.

(c) Basta observar la igualdad del apartado (a) precedente.

(d) De nuevo se sigue observando el apartado (a), ó bien directamente como se indica a continuación. Se tiene que $c'\alpha = c$, por lo que $c'\alpha\beta = c\beta$, es decir, $c_2' = c\beta$. Por otra parte, $c_1\alpha\beta = c$, luego $c_1\alpha = c\beta = c_2'$ como se quería.

(e) Teniendo en cuenta la expresión de γ como producto de ciclos disjuntos, emparejando ciclos de la misma longitud y aplicando a cada pareja el apartado (a), se tiene el resultado.

2.2. Descripción de la máquina mediante las permutaciones

A continuación se procede a explicar qué es lo que ocurre dentro de Enigma en términos de permutaciones tal y como lo hizo Rejewski.

Los cableados que entran y salen de cada elemento de la máquina tranforman una letra en otra. La idea es ver cada parte de la máquina como una permutación del conjunto:

$$C = \{a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z\}$$

Sea S la permutación correspondiente al clavijero, L, M y N las permutaciones de los rotores en una determinada posición, vistos de izquierda a derecha, y con la letra R la permutación correspondiente al reflector. Rejewski consideró una permutación más, esta permutación constituía el paso entre el clavijero y el rotor N, se trataba de un rotor fijo cuya permutación se denoto con la letra H, la cual vio más adelante que no era necesaria considerar. Por lo tanto, el circuito que sigue la corriente dentro de la máquina en una determinada posición de los rotores puede expresarse como:

$$SNMLRL^{-1}M^{-1}N^{-1}S^{-1}$$

Pero hay que tener en cuenta que después de pulsar una tecla, el rotor a la derecha, N, gira $\frac{1}{26}$ parte. Para tener en cuenta este movimiento se introdujo una nueva permutación, denominada con la letra P, la cual cambia cada letra por la siguiente según el orden alfabético. Por lo tanto, se puede representar la primera permutación que realiza un rotor, denotada por A, por la siguiente expresión:

$$A = SPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}S^{-1}$$

Suponiendo que solo gira el rotor de la derecha, N, es decir no se ha dado el turnover del rotor. En su trabajo, Rejewski indicó que la hipótesis de que solo girase el rotor derecho en las seis primeras permutaciones mientras que los otros dos rotores quedaban fijos, era válida, en promedio, en 21 casos de 26 posibles. De esta forma, se pueden describir las seis primeras permutaciones de la máquina, este es el primer paso a realizar para obtener el cableado de los rotores. Por lo tanto dichas seis permutaciones quedarían de la siguiente forma:

$$A = SPNP^{-1}MLRL^{-1}M^{-1}PN^{-1}P^{-1}S^{-1}$$

$$B = SP^2NP^{-2}MLRL^{-1}M^{-1}P^2N^{-1}P^{-2}S^{-1}$$

$$\dots$$

$$F = SP^6NP^{-6}MLRL^{-1}M^{-1}P^6N^{-1}P^{-6}S^{-1}$$

En estas ecuaciones, Rejewski observó una repetición de la permutación $MLRL^{-1}M^{-1}$, que sustituyó por la letra Q. Esto permitió simplificar las ecuaciones:

$$A = SPNP^{-1}QPN^{-1}P^{-1}S^{-1}$$

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

$$\dots$$

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

Por lo tanto, el problema que se le presento a Rejewski era resolver un sistema de seis ecuaciones con cuatro incógnitas, S, N y Q.

A lo largo del trabajo se va a usar la siguiente notación:

Rotor I	Rotor IV	Rotor V	Clavijero	Calvijero
λ	μ	ν	σ	ρ

Cifrar una letra con Enigma es lo mismo que aplicar a dicha letra una determinada permutación. Dicha permutación depende de las anteriormente nombradas, del orden de los rotores y del ajuste conjunto. La permutación que produce cada rotor depende del ajuste conjunto. Por ejemplo, el rotor I tiene 26 posiciones distintas que producen la permutacion $\pi^i\mu\pi^{-i}, i = 1,..,26$, siendo:

$$\pi = \{abcdefghijklmnopqrstuvwxyz\}$$

A la permutación que indica el funcionamiento de Enigma se denota por α y se llama Permutación Enigma. De forma más precisa, para una máquina Enigma cuyo orden de los rotores es I-IV-V y con posiciones absolutas (a, b, c) en el momento de presionar cualquier letra del teclado, la permutación α es:

$$\boxed{\alpha = \sigma\pi^{c+1}\nu\pi^{-c-1+b}\mu\pi^{-b+a}\lambda\pi^{-a}\rho\pi^{a}\lambda^{-1}\pi^{b-a}\mu^{-1}\pi^{c+1-b}\nu^{-1}\pi^{-c-1}\sigma}$$

En forma compacta

$$\boxed{\alpha = \sigma\nu^{\pi^{-c-1}}\mu^{\pi^{-b}}\lambda^{\pi^{-a}}\rho\lambda^{\pi^{a}}\mu^{\pi^{b}}\nu^{\pi^{c+1}}\sigma}$$

Supuesto que en ese momento el rotor central no se ha movido. Si se hubiera dado el caso contrario, se procedería aumentando una unidad el ajuste b, en el caso de que girara el rotor central, y el ajuste

a, en el caso de que girara el rotor de la izquierda. Es importante notar que la máquina Enigma realiza un paso antes de codificar, y por lo tanto si el ajuste conjunto inicial del rotor de la derecha es en c, la codificación tendra lugar en $c+1$.

La permutación ρ que representa la acción del reflector es un producto de 13 transposiciones disjuntas, es decir, se trata de una involución sin puntos fijos. Como ρ y α son conjugadas, por teoría de las permutaciones, α es también un producto de 13 transposiciones disjuntas, $\sigma = \sigma^{-1}$.

Si $x\alpha = y$ y $y\alpha = x$, esto justifica que una configuración exactamente igual de la máquina sirve para encriptar y desencriptar.

2.3. Máquina Enigma virtual y construcción de datos

Para la realización de este trabajo es necesario tener ciertos datos a modo de ejemplo para poder ir describiendo apropiadamente el proceso. Para la construcción de dichos datos se ha utilizado la máquina virtual Enigma Simulator v7.0. Se trata de un programa para el ordenador que simula la máquina Enigma Wehrmacht de tres rotores, la estudiada en este trabajo. También posee otros modelos que se usaron durante la Segunda Guerra Mundial de la máquina pero para este trabajo poco relevantes.

Construcción de los datos

Como ya se ha indicado, en este trabajo se va a seguir el procedimiento realizado por Rejewski para encontrar el cableado de los rotores de Enigma. Para ello se dispone, en un primer momento, de 30 cabeceras de mensajes cifrados con Enigma, al igual que tenía Rejewski.

Lo primero es elegir una configuración determinada de la máquina para poder tomar datos. La configuración utilizada es la siguiente:

Orden Rotores	Ajuste Rotores	Ajuste Conjunto	Clavijero	Reflector
I-IV-V	SPB TFG	(1,16,5)	(e n)(i g)(m a)(r w)(s k)(p b)	C

Una vez configurada la máquina con estos datos tecleamos las cabeceras seleccionadas, esto es, un conjunto de tres letras repetidas dos veces. Una vez tecleada una cabecera tenemos que asegurarnos de volver al ajuste inicial antes de teclear la siguiente cabecera.

La selección realizada de cabeceras tiene su explicación. Se supone que los soldados encargados en enviar mensajes tendían a repetir letras, ya fueran las tres de la terna o dos letras de la terna seguidas, o algunas letras relacionadas con algo.

Las tres letras que serviran luego de clave del mensaje

AAA	BBB	CCC	DDD	EEE	FFF
GGG	HHH	III	JJJ	KKK	LLL
MMM	NNN	OOO	PPP	QQQ	RRR
SSS	TTT	UUU	VVV	WWW	XXX
YYY	ZZZ	SAN	DRA	MAT	TFG

Cabeceras cifradas

YQS YYQ	TCI QXU	VBD RTW	HZC TGS	IYX SJG	ZIQ VMJ
UNK UDE	DUN NQX	EFB PUN	WTU LEF	QLG MPZ	SKV JOO
PPY KFY	XGH HRI	RSW XLL	MMZ IKT	KAF BHA	OWT CNV
LOA EVD	BJR DCP	GHJ GIB	CXL FSR	JRO ZZC	NVE OBH
AEM AAM	FDP WWK	LQH EYI	HWS TNQ	PQR KYP	BIK DME

Funcionamiento de la máquina

Esta máquina funciona exactamente igual que una máquina Enigma real. Se configura la máquina y a continuación se procede al cifrado del mensaje.

Figura 2.1: Escritorio de la máquina: 1-Ventanilla. 2-Lámparas. 3-Teclado. 4-Acceso al interior. 5- Acceso al clavijero.

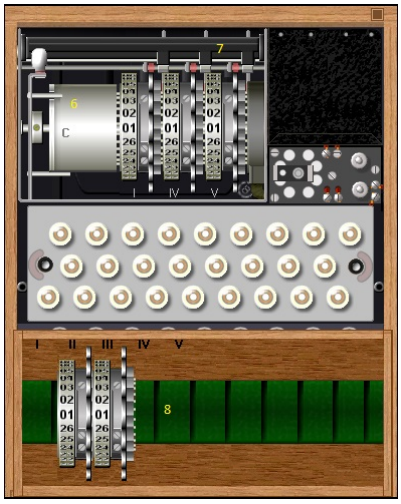

Figura 2.2: Interior de la máquina: 6-Reflector. 7-Eje de los rotores. 8-Rotores posibles.

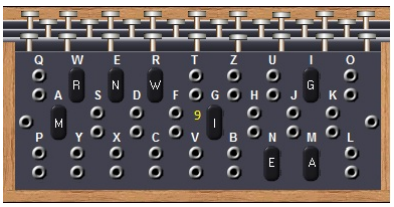

Figura 2.3: Clavijero: 9-Clavijero.

Capítulo 3

Encontrando el cableado de la Máquina Enigma y otros detalles

Este capítulo se centra en encontrar el cableado de los rotores y otros detalles mediante el uso de las permtuaciones y siguiendo el trabajo realizado por Rejewski.

3.1. Las seis primeras permutaciones

Rejewski se dio cuenta de que las seis primeras letras de una mensaje cifrado por la máquina eran tres letras repetidas. En efecto, son tres letras de la clave del mensaje que se transmitían dos veces para evitar errores. Cada letra de la clave y su repetición esta cifrada por una permutación, sea esta α_i con $i = 1, ..., 6$. Estas seis permutaciones α_i no variaban en un mismo día, ya que la máquina cifraba antes de ser configurada con la clave del mensaje suponiendo que el resto de la configuración de la máquina seguía siendo la misma. Como se ha observado anteriormente, cada una de estas permutaciones α_i es conjugada de la permutación ρ, permutación correspondiente al reflector. Por lo tanto cada α_i es una involución sin puntos fijos, es decir, se trata de un producto de trece transposiciones disjuntas.

Por ejemplo, suponer que la clave del mensaje es ABC y su correspondiente cabecera del mensaje es DEF GHI. Se observa que $A\alpha_1 = D$ y $A\alpha_4 = G$, es decir, la primera permutación que efectúa Enigma y la cuarta permutación mueven la letra A a dos letras diferentes, la D y la G. Recordar que dichas permutaciones se tratan de involuciones, por lo tanto:

$$G = A\alpha_4 = A\alpha_1\alpha_1\alpha_4 = D\alpha_1\alpha 4$$

Por lo tanto, se observa que $\alpha_1\alpha_4$ mueve la primera letra de cada cabecera a la que ocupa la cuarta posición. De forma análoga ocurre que $\alpha_2\alpha_5$ mueve la segunda letra a la quinta y $\alpha_3\alpha_6$ mueve la tercera a la sexta.

Para encontrar las seis primeras permutaciones realizadas por Enigma, Rejewski disponía de una colección grande de mensajes cifrados con la máquina, lo que le proporcionaba una cantidad suficiente de cabeceras con las que trabajar y encontrar las permutaciones deseadas. Se dispone de las siguientes treinta cabeceras cifradas:

YQK YYQ	MMZ IST	VPD RTW	HZC TGK	IYX KJG	ZIQ VMJ
UNS UDE	DUN NQX	EFP BUN	WTU LEF	LOA EVD	KSV JOO
BBY SFY	XGH HRI	RKW XLL	TCI QXU	SAF PHA	OWT CNV
QLG MBZ	PJR DCB	GHJ GIP	CXL FKR	JRO ZZC	NVE OPH
AEM AAM	FDB WWS	QQH MYI	HWK TNQ	BQR SYB	PIS DME

Comentar, que solamente se sabe que estas cabeceras provienen de la clave del mensaje y de su repetición, no es conocido ni cuales son las cabeceras originales ni la configuración de la máquina.

A partir de este conjunto de cabeceras y de haber deducido como mueven las permutaciones $\alpha_1\alpha_4$, $\alpha_2\alpha_5$ y $\alpha_3\alpha_6$ las letras de las cabeceras podemos saber los ciclos que forman dichos productos de

permutaciones. A continuación se ven tablas que muestras como la letra en la posición i-ésima es movida a la posición (i+3)-ésima y como se obtienen el producto de las permutaciones α pertinentes.

$\alpha_1\alpha_4$

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

$$\alpha_1\alpha_4 = (a)(g)(u)(y)(x\ h\ t\ q\ m\ i\ k\ j\ z\ v\ r)(b\ s\ p\ d\ n\ o\ c\ f\ w\ l\ e)$$

A partir de la tabla anterior se ve claramente que así es como tiene que ser este producto, ya que se puede seguir fácilmente que la m se mueve a la i (cuarta columna tercera fila),la i se mueve a la s (quinta columna primera fila) y así sucesivamente. Este proceso se usa para hallar los dos siguientes productos.

$\alpha_2\alpha_5$

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

$$\alpha_2\alpha_5 = (u\ q\ y\ j\ c\ x\ k\ l\ b\ f)(a\ h\ i\ m\ s\ o\ v\ p\ t\ e)(r\ z\ g)(n\ d\ w)$$

$\alpha_3\alpha_6$

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

$$\alpha_3\alpha_6 = (m)(y)(c\ k\ q\ j\ p\ n\ x\ g\ z\ t\ v\ o)(r\ b\ s\ e\ h\ i\ u\ f\ a\ d\ w\ l)$$

Se observa que se cumple el apartado b del teorema 2.5, cada ciclo aparece un número par de veces.

A continuación se procede a la obtención de cada permutación α.

Por el apartado c del teorema 2.5, se sabe que si un 2-ciclo, es decir una involución sin puntos fijos, pertenece a una permutación α_i entonces cada una de sus letras pertenecera a ciclos disjuntos de igual longitud.

Rejewski intuía que los criptógrafos alemanes usaban como claves de mensaje combinaciones de letras tipo AAA, BBB, ... Al final se comprobo que estas suposiciones eran ciertas gracias al éxito del trabajo de Rejewski.

Suponer como clave AAA. Por el apartado c del teorema 2.5 se sigue que:

$$A \xrightarrow{-\alpha_1} (g)(u)(y)$$

$$A \xrightarrow{-\alpha_2} (u\ q\ y\ j\ c\ x\ k\ l\ b\ f)$$

$$A \xrightarrow{-\alpha_3} (c\ k\ q\ j\ p\ n\ x\ g\ z\ t\ v\ o)$$

Luego entre el conjunto de cabeceras disponible hay que encontrar una tal que cada una de sus tres primeras letras pertenezca a las permutaciones escritas anteriormente, respectivamente.

YQK YYQ	MMZ IST	VPD RTW	HZC TGK	IYX KJG	ZIQ VMJ
UNS UDE	DUN NQX	EFP BUN	WTU LEF	LOA EVD	KSV JOO
BBY SFY	XGH HRI	RKW XLL	TCI QXU	SAF PHA	OWT CNV
QLG MBZ	PJR DCB	GHJ GIP	CXL FKR	JRO ZZC	NVE OPH
AEM AAM	FDB WWS	QQH MYI	HWK TNQ	BQR SYB	PIS DME

Ahora solo hay que ver cual de las treinta cabeceras tiene sus tres primeras letras pintadas. En este caso se trata de una única cabecera:

$$YQK\ YYQ$$

Esto indica lo siguiente:

$$\alpha_1 = (a\ y)... \ \alpha_2 = (a\ q)... \ \alpha_3 = (a\ k)...$$

$$\alpha_4 = (a\ y)... \ \alpha_5 = (a\ y)... \ \alpha_6 = (a\ q)...$$

Gracias al apartado d del teorema 2.5 se obtiene lo siguiente:

$$\alpha_1 = (a\ y)(g\ u)...$$

$$\alpha_2 = (a\ q)(h\ u)(i\ f)(m\ b)(s\ l)(o\ k)(v\ x)(p\ c)(t\ j)(e\ y)...$$

$$\alpha_3 = (a\ k)(d\ c)(w\ o)(l\ v)(r\ t)(b\ z)(s\ g)(e\ x)(h\ n)(i\ p)(u\ j)(f\ q)...$$

$$\alpha_4 = (a\ y)(g\ u)...$$

No son necesarias α_5 y α_6 para el resto del proceso, por lo tanto se dejan sin calcular aunque el proceso es análogo a la obtención del resto de permutaciones.

Con este primer paso hemos obtenido muchas trasposiciones pertenecientes a las permutaciones que se desea encontrar. Pero aún falta hallar las restantes. Para ello se repite el proceso pero suponiendo que se ha tomado otra cabecera distinta a la anterior.

Se observa claramente que el ciclo que falta de encontrar para α_3 es el ciclo compuesto por $(y\ m)$, ya que como afirma el apartado c del teorema 2.5, las dos letras que componen el 2-ciclo perteneciente a una permutación α_i deben pertenecer a ciclos disjuntos de igual longitud. En la composición de permutaciones $\alpha_3\alpha_6$ solo existen dos 1-ciclos, por lo tanto es claro que ambos formaran un 2-ciclo.

Para acabar de conseguir todas las trasposiciones de las permutaciones, suponer una vez más que se usa una cabecera. En este caso suponer usada la cabecera ZZZ.

$$Z \xrightarrow{\alpha_1} (b\ s\ p\ d\ n\ o\ c\ f\ w\ l\ e)$$

$$Z \xrightarrow{\alpha_2} (n\ d\ w)$$

$$Z \xrightarrow{\alpha_3} (r\ b\ s\ e\ h\ i\ u\ f\ a\ d\ w\ l)$$

YQK YYQ	MMZ IST	VPD RTW	HZC TGK	IYX KJG	ZIQ VMJ
UNS UDE	DUN NQX	EFP BUN	WTU LEF	LOA EVD	KSV JOO
BBY SFY	XGH HRI	RKW XLL	TCI QXU	SAF PHA	OWT CNV
QLG MBZ	PJR DCB	GHJ GIP	CXL FKR	JRO ZZC	NVE OPH
AEM AAM	FDB WWS	QQH MYI	HWK TNQ	BQR SYB	PIS DME

Cabecera resultante:

$$FDB\ WWS$$

Por lo tanto:

$$\alpha_1 = (z\ f)... \ \alpha_2 = (z\ d)... \ \alpha_3 = (z\ b)...$$

$$\alpha_4 = (z\ w)... \ \alpha_5 = (z\ w)... \ \alpha_6 = (z\ s)...$$

Así se consigue los ciclos restantes:

$$\alpha_1 = (d\ h)(t\ p)(q\ s)(m\ b)(i\ e)(k\ l)(j\ w)(z\ f)(v\ c)(r\ o)(x\ n)$$

$$\alpha_2 = (r\ w)(z\ d)(g\ n)$$

$$\alpha_4 = (d\ t)(q\ p)(m\ s)(i\ b)(k\ e)(j\ l)(z\ w)(v\ f)(r\ c)(x\ o)(h\ n)$$

Por lo tanto se obtiene las cuatro primeras permutaciones realizadas por la máquina Enigma:

$$\boxed{\alpha_1 = (a\ y)(g\ u)(k\ l)(j\ w)(z\ f)(v\ c)(r\ o)(x\ n)(h\ d)(t\ p)(q\ s)(m\ b)(i\ e)}$$

$$\boxed{\alpha_2 = (r\ w)(z\ d)(g\ n)(a\ q)(h\ u)(i\ f)(m\ b)(s\ l)(o\ k)(v\ x)(p\ c)(t\ j)(e\ y)}$$

$$\boxed{\alpha_3 = (y\ m)(a\ k)(d\ c)(w\ o)(l\ v)(r\ t)(b\ z)(s\ g)(e\ x)(h\ n)(i\ p)(u\ j)(f\ q)}$$

$$\boxed{\alpha_4 = (k\ e)(j\ l)(z\ w)(v\ f)(r\ c)(x\ o)(h\ n)(t\ d)(q\ p)(m\ s)(i\ b)(a\ y)(g\ u)}$$

Con estas permutaciones se pueden encontrar todas las claves del mensaje que enviaba el correspodiente soldado. Esto daba pistas para las de otro día y es fácil encontrar $\alpha_1, \alpha_2, \alpha_3$ y α_4 de cada día.

3.2. Cableado de los rotores IV y V, salvo torsión

Recordar el modelo matemático que refleja el funcionamiento de la máquina:

$$\boxed{\alpha = \sigma\pi^{c+1}\nu\pi^{-c-1+b}\mu\pi^{-b+a}\lambda\pi^{-a}\rho\pi^{a}\lambda^{-1}\pi^{b-a}\mu^{-1}\pi^{c+1-b}\nu^{-1}\pi^{-c-1}\sigma}$$

En este punto de su estudio, Rejewski poseía el modelo matemático que refleja el funcionamiento interno de la máquina, un ejemplo de un mensaje cifrado con Enigma, las permutaciones iniciales que generaba Enigma a lo largo de cada día de Septiembre y Octubre de 1932, las posiciones absolutas y la configuración del clavijaero de cada uno de los días mencionados y el orden de los rotores de ambos dos meses, estos últimos datos los obtuvo del cuaderno de claves que le fue proporcionado.

Se va a usar uno de los días que aparecen en el cuaderno de claves:

Orden Rotores	Ajuste Rotores	Ajuste Conjunto	Clavijero
I-IV-V	SPB TFG	(1,16,5)	(e n)(i g)(m a)(r w)(s k)(p b)

Considerando solamente las cuatro primeras permutaciones y la configuración descrita se deduce:

$$\alpha_i = \sigma\pi^{c+i}\nu\pi^{-c-i}\chi\pi^{c+i}\nu^{-1}\pi^{-c-i}\sigma,\ i = 1,2,3,4$$

Donde χ representa la acción conjunta del reflector, el rotor central y el rotor de la izquierda. La permutación $\chi = \pi^{b}\mu\pi^{-b+a}\lambda\pi^{-a}\rho\pi^{a}\lambda^{-1}\pi^{b-a}\mu^{-1}\pi^{-b}$ es la misma para las cuatro expresiones, asumiendo que el rotor central no se mueve entre la segunda y a cuarta permutación. Hay que encontrar ν con α_i y c conocidas.

Sea $\beta_i = \pi^{-c-i}\sigma\alpha_i\sigma\pi^{c+i} = \alpha_i^{\sigma\pi^{c+i}}$, i=1,...,4. Por lo tanto $\beta_i^{\nu\pi^{-c-i}} = \chi$.
Como χ no varía de una perutación a la siguiente se puede igualar:

$$\beta_i^{\nu\pi^{-c-i}} = \beta_{i+1}^{\nu\pi^{-c-i-1}}$$

Como $\pi^{-c-i}\pi^{c+i+1} = \pi$, se sigue:

$$\beta_i^{\nu\pi} = \beta_{i+1}^{\nu}$$

$$\beta_i^{\nu\pi\nu^{-1}} = \beta_{i+1}$$

Sea $\gamma = \pi^{-\nu^{-1}}$, luego

$$\boxed{\beta_i^{\gamma} = \beta_{i+1}}$$

Esta fórmula solo sirve para las seis primeras permutaciones, es decir, en el proceso de introducción de la clave del mensaje, ya que luego el ajuste externo varía.

Ahora se procede a calcular las permutaciones β_i.

$$\beta_1 = \alpha_1^{\sigma\pi^6}$$

$$\beta_2 = \alpha_2^{\sigma\pi^7}$$
$$\beta_3 = \alpha_3^{\sigma\pi^8}$$
$$\beta_4 = \alpha_4^{\sigma\pi^9}$$

Donde las permutaciones α_i y σ son conocidas. Las potencias de π se calculan facilmente obteniendo:

$$\pi^6 = (a\ g\ m\ s\ y\ e\ k\ q\ w\ c\ i\ o\ u)(b\ h\ n\ t\ z\ f\ l\ r\ x\ d\ j\ p\ v)$$
$$\pi^7 = (a\ h\ o\ v\ c\ j\ q\ x\ e\ l\ s\ z\ g\ n\ u\ b\ i\ p\ w\ d\ k\ r\ y\ f\ m\ t)$$
$$\pi^8 = (a\ i\ q\ y\ g\ o\ w\ e\ m\ u\ c\ k\ s)(b\ j\ r\ z\ h\ p\ x\ f\ n\ v\ d\ l\ t)$$
$$\pi^9 = (a\ j\ s\ b\ k\ t\ c\ l\ u\ d\ m\ v\ e\ n\ w\ f\ o\ x\ g\ p\ y\ h\ q\ z\ i\ r)$$

Realizando las operaciones pertinentes se llega a:

$$\beta_1 = (s\ e)(o\ a)(y\ r)(p\ x)(f\ l)(b\ i)(c\ u)(d\ k)(n\ j)(z\ h)(w\ q)(g\ v)(m\ t)$$
$$\beta_2 = (t\ x)(o\ b)(n\ m)(h\ w)(r\ s)(v\ z)(c\ e)(i\ j)(a\ q)(u\ f)(d\ y)(g\ k)(p\ l)$$
$$\beta_3 = (u\ a)(l\ k)(z\ w)(t\ d)(e\ b)(x\ h)(s\ q)(v\ f)(p\ m)(o\ j)(c\ r)(n\ y)(g\ i)$$
$$\beta_4 = (v\ h)(r\ d)(b\ w)(s\ u)(i\ a)(e\ o)(f\ l)(g\ x)(q\ n)(c\ m)(z\ k)(j\ t)(p\ y)$$

Una vez calculadas β_i, se debe encontrar una única γ tal que:

$$\beta_i^\gamma = \beta_{i+1}$$

Notar que γ se trata de la permutación que conjuga β_i a β_{i+1}. También hay que tener en cuenta que la γ buscada se trata de un 26-ciclo, lo cual acorta el hecho de buscarla. Un proceso de obtener conjugados es poner los ciclos de misma longitud uno encima del otro y ver que permutación se obtiene. Hay que tener en cuanta que se trata de encontrar una única γ que conjugue cuatro permutaciones, por lo tanto se debe realizar el proceso anterior pero poniendo las β_i una encima de la otra y ver que no se cometa ninguna contradicción en el proceso.
Se procede entonces dejando fija una de las permutaciones, la β_1, y debajo de esta se va probando con las restantes letras del alfabeto. Además, para ver que se trata de una permutación única se debe probar que con el resto de letras no se genera ninguna permutación conjugada.
Puede ocurrir que existan varias γ que conjuguen pero se sabe que la buscada es un 26-ciclo y solo habra una solución que cumpla todo lo pedido.
Se va proceder viendo a que letra se puede mover la letra a.

a $\rightarrow$ **b**

β_1	(ao)	(gv)	(qw)		(hz)		
β_2	(bo)	(aq)	(ec)	(wh)	(rs)	(zv)	(gk)
β_3		(be)	(dt)	(cr)	(jo)	(sq)	(au)
β_4		(rd)		(tj)		(oe)	

Se observa una contradicción, ya que la letra r viene de dos letras diferentes. Por lo tanto de aquí no se va a obtener la γ buscada. Además se observa que se produciría un 1-ciclo en la permutación buscada ya que $o \rightarrow o$.
Se procede de igual manera hasta que una tabla no muestra ninguna contradicción.

La tabla que ofrece la γ buscada es la siguiente:

a $\rightarrow$ **r**

β_1	(ao)	(ib)	(qw)	(xp)	(gv)	(uc)	(jn)	(fl)	(dk)	(hz)	(tm)	(es)	(ry)
β_2	(rs)	(aq)	(ce)	(wh)	(ij)	(dy)	(uf)	(tx)	(kg)	(bo)	(zv)	(nm)	(pl)
β_3	(pm)	(rc)	(yn)	(eb)	(au)	(kl)	(dt)	(zw)	(gi)	(qs)	(oj)	(fv)	(hx)
β_4	(hv)	(py)	(lf)	(nq)	(rd)	(gx)	(kz)	(oe)	(ia)	(cm)	(su)	(tj)	(bw)

$$\boxed{\gamma = (a\ r\ p\ h\ b\ q\ c\ y\ l\ x\ w\ e\ n\ f\ t\ z\ o\ s\ m\ v\ j\ u\ d\ k\ g\ i)}$$

Al comprobar con todas las letras posibles que esta es la única que no da contradicciones, se prueba que esta γ es la única permutación que conjuga β_i a β_{i+1}. Si el rotor central girase por efecto del rotor derecho sería indicativo de que la permutación buscada no existe. Si se diese la situación de que existieran dos γ 26-ciclos que conjugasen β_i y β_{i+1}, no se tendrían datos suficientes, sería necesario buscar una β_i más.

Por último, falta encontrar ν_0, permutación perteneciente al rotor de la derecha sin tener en cuenta la torsión de este. Esto es, una vez obtenida la permutación γ, se tiene que computar una de las 26 permutaciones posibles que conjugan γ a π, ya que $\gamma = \pi^{-\nu^{-1}}$. Se realiza el mismo proceso anterior definido, proceso que consiste en poner una permutación encima de la otra. Suponer que la letra a se queda fija.

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

Por lo tanto, una de las 26 posibles permutaciones es:

$$\nu_0 = (a)(b\ e\ l\ i\ z\ p\ c\ g\ y\ h\ d\ w\ k\ x\ j\ u\ v\ t\ o\ q\ f\ n\ m\ s\ r)$$

Por el teorema 2.4, se deduce que la permutación que define al rotor de la derecha, V, salvo torsión es:

$$\boxed{\nu = \nu_0\pi^n, n \in 0,...,26}$$

Como se ha indicado anteriormente, en este trabajo se sigue el trabajo realizado por Rejewski. Él poseía datos de dos meses diferentes, en este caso se esta suponiendo que durante esos dos meses de los que se tienen datos la posición del rotor central y derecho se intercambio, es decir, en un mes el orden de los rotores era I-IV-V y en el otro mes I-V-IV, por lo tanto con un proceso análogo al realizado con el rotor de la derecha se puede proceder para encontrar el cableado del rotor central, IV, salvo torsión.

Tomado como configuración de la máquina:

Orden Rotores	Ajuste Rotores	Ajuste Conjunto	Clavijero
I-V-IV	SAN PBA	(23, 1, 13)	(e n)(i g)(m a)(r w)(s k)(p b)

Y así obtener:

$$\mu_0 = (a)(b\ o\ t\ c\ k\ q\ j\ m\ n\ d\ r)(e\ l)(f\ v\ z\ x\ i\ u\ g)(h\ w\ y\ s\ p)$$

$$\boxed{\mu = \mu_0\pi^m, m \in 0,...,26}$$

3.3. Torsión de los rotores IV y V

Una vez obtenida una de las 26 posibles permutaciones que rigen al rotor derecho, falta ver cual es exactamente, es decir hay que encontrar la torsión de dicho rotor.

Rejewski aplazó el estudio de las torsiones sin explicar como lo hace. En este trabajo se va a mostrar como es posible deducir la torsión del rotor de la derecha usando las claves de dos días. Este proceso es seguido por Paz Jiménez y Manuel Vázquez en sus trabajos [5] [6].

Mediante el trabajo ya realizado en 3.2 se ha obtenido una de las 26 posibles permutaciones del rotor de la derecha, rotor V, dada por:

$$\nu = \nu_0\pi^n, n \in 0,...,26$$

Esto es, se debe hallar el valor de n.

Para poder realizar este proceso es necesario tener datos de dos días del mismo mes, con posiciones absolutas (a,b,c) y (a,b',c') respectivamente, con $b \neq b'$, y se denota por α y α' a la primera permutación realizada por la máquina cada uno de los dos días seleccionados. Estas dos últimas permutaciones nombradas se obtienen mediante el procedimiento realizado anteriormente. Notar que la primera cifra de ambas posiciones absolutas es la misma, ya que solo hay 26 posibles valores para a y en un mes hay mínimo 30 días, por lo tanto es claro que existen dos posiciones absolutas con igual valor de a.

Teniendo en mente el modelo matemático que refleja el funcionamiento de la máquina:

$$\boxed{\alpha = \sigma\pi^{c+1}\nu\pi^{-c-1+b}\mu\pi^{-b+a}\lambda\pi^{-a}\rho\pi^{a}\lambda^{-1}\pi^{b-a}\mu^{-1}\pi^{c+1-b}\nu^{-1}\pi^{-c-1}\sigma}$$

La ecuación correspondiente al segundo día tomado sería:

$$\alpha' = \sigma'\pi^{c'+1}\nu_0\pi^{-c'-1+b'}\pi^{n}\mu_0\pi^{-b'}\pi^{a+m}\lambda\pi^{-a}\rho\pi^{a}\lambda^{-1}\pi^{-m-a}\pi^{b'}\mu_0^{-1}\pi^{-n}\pi^{c'+1-b'}\nu_0^{-1}\pi^{-c'-1}\sigma'$$

Esta segunda ecuación corresponde a la configuración:

Orden Rotores	Ajuste Rotores	Ajuste Conjunto	Clavijero
I-IV-V	SPB TVX	(1,6,22)	(r e)(j w)(s k)(y a)(n d)(p b)

Se denotan los siguientes grupos de operaciones entre permutaciones de la siguiente manera:

$$\tau = \sigma\pi^{c+1}\nu_0\pi^{-c-1+b}$$

$$\eta = \mu_0\pi^{-b}\pi^{b'}\mu_0^{-1}$$

$$\chi = \pi^{a+m}\lambda\pi^{-a}\rho\pi^{a}\lambda^{-1}\pi^{-m-a}$$

Se tiene como incógnitas las permutaciones π^n y χ.

Sea $\beta = \pi^{c+1}\nu_0^{-1}\pi^{-c-1}\sigma\alpha\sigma...\pi^{-c-1+b} = \tau^{-1}\alpha\tau = \alpha^{\tau}$. Y de forma análoga se obtiene la fórmula para β'.

Por lo tanto, operando convenientemente se obtiene:

$$\pi^{n}\mu_0\pi^{-b}\chi\pi^{b}\mu_0^{-1}ß^{-n} = \alpha^{\tau} = \beta$$

$$\chi^{\pi^{b}\mu_0^{-1}\pi^{-n}} = \beta$$

$$\beta^{\pi^{b}\mu_0\pi^{-n}} = \chi$$

Como χ es la misma para ambos días, se tiene:

$$\beta^{\pi^{b}\mu_0\pi^{-n}} = \beta'^{\pi^{b'}\mu_0\pi^{-n}}$$

$$\beta^{\eta^{\pi^{-n}}} = \beta'$$

Por lo tanto tenemos que encontrar una tal n que cumpla la igualdad anterior.

Para ello se necesitan las permutaciones: α, α', ν_0, μ_0 y calcular las permutaciones: τ, τ', β, β', η.

Calculo de τ y β

Primero se procede calculando:

$$\tau = \sigma\pi^{c+1}\nu_0\pi^{-c-1+b}$$

En este caso: $b = 16$ y $c = 5$.

σ	(e n)(i g)(m a)(r w)(s k)(p b)
π^6	(a g m s y e k q w c i o u)(b h n t z f l r x d j p v)
ν_0	(a)(b e l i z p c g y h d w k x j u v t o q f n m s r)
π^{10}	(a k u e o y i s c m w g q)(l v f p z j t d n x h r b)

Por lo tanto:

$$\tau = (a\ b\ d\ e\ y\ v\ o\ f\ s\ p\ n\ h\ w\ t\ z\ x\ g)(c\ j\ m\ i)(r\ q\ u\ k)(l)$$

Una vez obtenida la permutación τ, se procede a obtener

$$\beta = \alpha^{\tau}$$

α	(a y)(g u)(s l)(j w)(z f)(v c)(r o)(x n)(h d)(t b)(q k)(m p)(i e)
τ	(a b d e y v o f s p n h w t z x g)(c j m i)(r q u k)(l)

Obteniendo así:

$$\beta = (b\ v)(a\ k)(r\ l)(m\ t)(x\ s)(o\ j)(q\ f)(g\ h)(w\ e)(z\ n)(u\ p)(i\ d)(c\ y)$$

Calculo de τ' y β'

Se trata del mismo proceso anterior pero con distinta configuración, ahora $b' = 6$ y $c' = 22$.

σ	(r e)(j w)(s k)(y a)(n d)(p b)
π^{23}	(x u r o l i f c z w t q n k h e b y v s p m j g d a)
ν_0	(a)(b e l i z p c g y h d w k x j u v t o q f n m s r)
π^{-17}	(a j s b k t c l u d m v e n w f o x g p y h q z i r)

$$\tau' = (a\ c\ y\ s\ m\ d\ g\ f\ p\ q\ v)(b)(j\ x\ e\ z\ t\ o\ r\ n)(h\ u\ k\ l\ i\ w)$$

α'	(a h)(b g)(c i)(d j)(e x)(f r)(k z)(l o)(m p)(n v)(q t)(s w)(u y)
τ'	(a c y s m d g f p q v)(b)(h u k l i)(j x e z t o r n)

$$\beta' = (c\ u)(q\ f)(y\ w)(j\ x)(z\ e)(p\ n)(l\ t)(i\ r)(d\ b)(g\ a)(v\ o)(m\ h)(k\ s)$$

Calculo de η

Para este caso se necesitan de las posiciones absolutas $b = 16$ y $b' = 6$

$$\eta = \mu_0 \pi^{-b} \pi^{b'} \mu_0^{-1}$$

μ_0	(a)(b o t c k q j m n d r)(e l)(f v z x i u g)(h w y s p)
π^{10}	(a k u e o y i s c m w g q)(l v f p z j t d n x h r b)
π^{6}	(a g m s y e k q w c i o u)(b h n t z f l r x d j p v)
μ_0^{-1}	(a)(r d n m j q k c t o b)(l e)(g u i x z v f)(p s y w h)

$$\eta = (a\ k\ u\ h\ j\ t\ y\ x\ w\ b\ l\ i\ c)(d\ p\ z\ m\ n\ o\ q\ v\ s\ g\ f\ e\ r)$$

Calculo de la torsión n

Una vez obtenidas todas las permutaciones necesarias se procede ya a la obtención de la torsión del rotor derecho. Tenemos que encontrar la única $n \in \{0, ..., 26\}$ tal que

$$\beta^{\eta^{\pi^{-n}}} = \beta'$$

Para ello hay que ir probando con distintos valores de n hasta que encontremos la igualdad buscada.

En este caso se trata de $n = 21$

π^{-21}	(a f k p u z e j o t y d i n s x c h m r w b g l q v)
$\eta^{\pi^{-21}}$	(f p z m o y d c b g q n h)(i u e r s t v a x l k j w)

$$\beta^{\eta^{\pi^{-21}}} = (g\ a)(x\ j)(s\ k)(o\ v)(l\ t)(y\ w)(n\ p)(q\ f)(i\ r)(m\ h)(e\ z)(u\ c)(b\ d) = \beta'$$

Por lo tanto:

$$\boxed{\nu = \nu_0 \pi^{21} = (a\ v\ o\ l\ d\ r\ w\ f\ i\ u\ q)(b\ z\ k\ s\ m\ n\ h\ y\ c)(e\ g\ t\ j\ p\ x)}$$

Mediante un proceso análogo se obtiene la torsión del rotor central, m. Todo esto es posible por la posición de los rotores en los dos meses de los cuales se tienen datos. Así $m = 4$

$$\boxed{\mu = \mu_0 \pi^4 = (a\ e\ p\ l\ i\ y\ w\ c\ o\ x\ m\ r\ f\ z\ b\ s\ t\ g\ j\ q\ n\ h)(d\ v)(k\ u)}$$

3.4. Cableado del rotor I, salvo torsión

Recordar el modelo matemático que refleja el funcionamiento de la máquina:

$$\boxed{\alpha = \sigma\pi^{c+1}\nu\pi^{-c-1+b}\mu\pi^{-b+a}\lambda\pi^{-a}\rho\pi^{a}\lambda^{-1}\pi^{b-a}\mu^{-1}\pi^{c+1-b}\nu^{-1}\pi^{-c-1}\sigma}$$

Se procede al calculo del cableado del rotor izquierdo, en este caso el rotor I, salvo torsión.
En este punto del trabajo, ν y μ son conocidas.
Se denota la siguente operación entre permutaciones de la siguiente manera:

$$\tau = \sigma\pi^{c+1}\nu\pi^{-c-1}\pi^{b}\mu\pi^{-b}\pi^{a}$$

Para encontrar el cableado del rotor I es necesaria la configuración de tres días del mismo mes, cosa que es fácil obtener ya que se poseen las claves de dos meses diferentes, con posiciones absolutas:

$$(a,\ b_1,\ c_1)$$

$$(a+r,\ b_2,\ c_2)$$

$$(a+2r,\ b_3,\ c_3)$$

$$(a+3r,\ b_4,\ c_4)$$

Donde $0 < r \leq 25$ es relativamnete primo con 26, y la suma $a+ir$ se entiende como una suma modulo 26.

Por lo tanto, se deduce:

$$\alpha_i = \tau_i\nu\pi^{-a-ri}\rho\pi^{a+ri}\nu^{-1}\tau_i^{-1},\ i = 1,2,3,4$$

La relación existente entre cada una de estas α_i y su anterior viene dada por:

$$\eta = \pi^{r}$$

Denotando como en ocasiones anteriores:

$$\beta_i = \tau_i^{-1}\alpha_i\tau_i,\ i = 1,2,3,4$$

Con las ecuaciones anteriores se obtiene el siguiente sistema a resolver:

$$\beta_i = \beta_{i-1}^{\gamma},\ i = 1,2,3,4$$

$$\gamma^{\lambda} = \pi^{r}$$

Con incógnitas γ y λ. Una forma efectiva de obtener γ es mediante las siguientes ecuaciones:

$$\delta_1 = \delta_0^{\gamma}$$

$$\delta_2 = \delta_1^{\gamma}$$

donde $\delta_i = \beta_i\beta_{i+1},\ i = 1,2,3,4$.

Como sucedía a la hora de encontrar el cableado de los otros dos rotores en 3.2, operando de esta forma y usando al teorema 2.4, se deduce que el cableado del rotor I, salvo torsión, viene dado por la permutación:

$$\lambda = \lambda_0\pi^{l},\ 0 \leq l \leq 25$$

Ahora se procede al calculo de λ_0.

Las configuraciones utilizadas son:

Orden Rotores	Ajuste Rotores	Ajuste Conjunto	Clavijero
I-IV-V	SPB TFG	(1,16,5)	(e n)(i g)(m a)(r w)(s k)(p b)

Orden Rotores	Ajuste Rotores	Ajuste Conjunto	Clavijero
I-IV-V	SPB CAS	(10,11,17)	(r e)(j w)(s k)(y a)(n d)(p b)

Orden Rotores	Ajuste Rotores	Ajuste Conjunto	Clavijero
I-IV-V	SPB LIA	(19,19,25)	(z a)(r g)(o h)(u e)(s c)(t l)

Orden Rotores	Ajuste Rotores	Ajuste Conjunto	Clavijero
I-IV-V	SPB URD	(2,2,2)	(s c)(a t)(e r)(u l)(g o)(n p)

Mediante el proceso explicado para obtener las seis primeras permutaciones en 3.1, se obtiene la primera permutación que genera la máquina cada uno de los cuatro días:

$$\alpha_1 = (a\ y)(g\ u)(k\ l)(j\ w)(z\ f)(v\ c)(r\ o)(x\ n)(h\ d)(t\ p)(q\ s)(m\ b)(i\ e)$$
$$\alpha_2 = (a\ o)(p\ c)(n\ u)(e\ r)(f\ z)(g\ s)(h\ q)(i\ d)(j\ k)(l\ t)(m\ y)(b\ v)(w\ x)$$
$$\alpha_3 = (a\ k)(b\ o)(s\ n)(d\ z)(e\ w)(f\ v)(g\ l)(h\ m)(i\ y)(j\ p)(t\ c)(q\ u)(r\ x)$$
$$\alpha_4 = (a\ q)(b\ u)(c\ l)(d\ i)(e\ m)(f\ w)(o\ s)(h\ p)(j\ t)(k\ r)(g\ z)(v\ n)(x\ y)$$

El siguiente paso a realizar es el obtener las correspondientes τ_i para cada una de las α_i:

$$\tau_1 = \sigma_1\pi^6\nu\pi^{20}\pi^{16}\mu\pi^{10}\pi = (a\ n\ z\ e\ r\ t\ v\ b\ h\ q\ w\ i\ x\ d\ m\ g\ o\ p\ j\ l\ u\ k\ c)(f\ s)(y)$$
$$\tau_2 = \sigma_2\pi^{18}\nu\pi^{8}\pi^{11}\mu\pi^{15}\pi^{10} = (a\ f\ l\ t\ b\ e\ x\ m)(n\ z\ k\ h\ u\ i\ w\ s\ j\ o\ q\ g\ c\ p)(r\ v\ d)(y)$$
$$\tau_3 = \sigma_3\pi^{0}\nu\pi^{0}\pi^{19}\mu\pi^{7}\pi^{19} = (a\ v)(b\ t\ c\ z\ x\ m\ j\ y\ d\ u)(o\ f\ s\ k\ i\ h\ p\ n\ e\ q\ g\ l)(r)(w)$$
$$\tau_4 = \sigma_4\pi^{3}\nu\pi^{23}\pi^{2}\mu\pi^{24}\pi^{2} = (a\ p\ b\ z\ e\ l\ v\ s)(i\ o\ x\ k\ j\ r\ m\ c\ h\ f\ g\ d\ t\ n)(q\ y\ w)(u)$$

Se sigue calculando β_i:

$$\beta_1 = \tau_1^{-1}\alpha_1\tau_1 = (a\ b)(c\ u)(d\ z)(e\ s)(f\ w)(g\ h)(i\ l)(j\ v)(k\ o)(m\ q)(n\ y)(p\ t)(r\ x)$$
$$\beta_2 = \tau_2^{-1}\alpha_2\tau_2 = (a\ y)(b\ t)(c\ j)(d\ e)(f\ q)(g\ u)(h\ o)(i\ z)(k\ l)(m\ s)(m\ p)(r\ w)(v\ x)$$
$$\beta_3 = \tau_3^{-1}\alpha_3\tau_3 = (a\ s)(b\ g)(c\ z)(d\ h)(e\ k)(f\ t)(i\ v)(j\ p)(l\ o)(m\ r)(n\ y)(q\ w)(u\ x)$$
$$\beta_4 = \tau_4^{-1}\alpha_4\tau_4 = (a\ x)(b\ f)(c\ l)(d\ e)(g\ q)(h\ v)(i\ s)(j\ m)(k\ w)(n\ r)(o\ t)(p\ y)(u\ z)$$

Observar que este proceso es similar al proceso realizado en el apartado 3.2 para calcular el cableado de los otros rotores salvo torsión, exceptuando que en este caso se utiliza cuatro configuraciones distintas de la máquina y las α_i son de cada uno de los cuatro días distintos.

El calculo de las δ_i no es necesario, pero facilita los calculos para obtener γ. Se calculan δ_i:

$$\delta_1 = \beta_1\beta_2 = (a\ t\ n)(b\ y\ p)(c\ g\ o\ l\ z\ e\ m\ f\ r\ v)(d\ i\ k\ h\ u\ j\ x\ w\ q\ s)$$
$$\delta_2 = \beta_2\beta_3 = (d\ k\ o)(e\ h\ l)(a\ n\ j\ z\ v\ u\ b\ f\ w\ m)(c\ p\ y\ s\ r\ q\ t\ g\ x\ i)$$
$$\delta_3 = \beta_3\beta_4 = (j\ y\ r)(m\ n\ p)(a\ i\ h\ e\ w\ g\ f\ o\ c\ u)(b\ q\ k\ d\ v\ s\ x\ z\ l\ t)$$

Ahora, hay que obtener una única γ tal que $\delta_i = \delta_{i-1}^{\gamma}$. El proceso para encontrarla es el mismo utilizado para obtener γ en 3.2. Solo que en este caso hay que fijarse en la longitud de los ciclos ya que una letra perteneciente a un ciclo de una determinada dimensión solo puede conjugarse a un ciclo de la misma dimensión que el que pertenece. Además, observar que γ es un 26-ciclo, lo que indica que no puede haber 1-ciclos, es decir, una letra no puede conjugarse a ella misma.

Observamos que la letra a de δ_1 puede ir a las letras d,k,o,e,h,l de δ_2, y la letra a de δ_2 puede ir a esas mismas letras en δ_3.

Por último, observar que para ver que se trata de una permutación única se debe probar que con el resto de letras no se genera ninguna permutación conjugada.

a $\rightarrow$ **d**

δ_1	(a t n)	
δ_2	(d k o)	(a n j z v u b f w m)
δ_3		(d v s x z l t b q k)

Se observa una contradicción ya que la letra *k* proviene de dos letras distintas.

Se procede de igual manera hasta que una tabla no muestra ninguna contradicción.
La tabla que ofrece la γ buscada es la siguiente:

a $\rightarrow$ **k**

δ_1	(a t n)	(i k h u j x w q s d)	(b y p)	(l z e m f r v c g o)
δ_2	(k o d)	(a n j z v u b f w m)	(l e h)	(y s r q t g x i c p)
δ_3	(n p m)	(k d v s x z l t b q)	(y r j)	(e w g f o c u a i h)

$$\boxed{\gamma = (a\ k\ n\ d\ m\ q\ f\ t\ o\ p\ h\ j\ v\ x\ u\ z\ s\ w\ b\ l\ y\ e\ r\ g\ c\ i)}$$

Al comprobar con todas las letras posibles que esta es la única que no da contradicciones, se prueba que esta γ es la única permutación que conjuga δ_i a $\delta i+1$.

Para acabar con el calculo de λ_0, una vez obtenida la permutación γ, se tiene que computar una de las 26 permutaciones posibles que conjugan γ a $\pi^r = \pi^9$, ya que $\gamma = \pi^{9(-\lambda^{-1})}$. Para ello se coloca una permutación encima de la otra. Suponer que la letra a se queda fija.

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

Por lo tanto, una de las 26 posibles permutaciones es:

$$\lambda_0 = (a)(b\ g\ z\ f\ c\ i\ r\ q\ t\ l\ p\ d)(e\ h\ m\ k\ j\ v)(n\ s\ o\ u\ w\ x)(y)$$

Por el teorema 2.4, se deduce que la permutación que define al rotor de la izquierda, I, salvo torsión es:

$$\boxed{\lambda = \lambda_0\pi^l, l \in 0,...,26}$$

3.5. Cableado del reflector, salvo conjugación

En esta sección se va a estudiar el cableado del reflector, en este caso se trata del reflector *C*.

Recordar el modelo matemático que refleja el funcionamiento de la máquina:

$$\boxed{\alpha = \sigma\pi^{c+1}\nu\pi^{-c-1+b}\mu\pi^{-b+a}\lambda\pi^{-a}\rho\pi^{a}\lambda^{-1}\pi^{b-a}\mu^{-1}\pi^{c+1-b}\nu^{-1}\pi^{-c-1}\sigma}$$

Tomando $\lambda = \lambda_0\pi^l$, para cualquier clave de día dada.

$$\alpha = \sigma\pi^{c+1}\nu\pi^{-c-1}\pi^{b}\mu\pi^{-b}\pi^{a}\lambda_0\pi^{l}\pi^{-a}\rho\pi^{a}\pi^{-l}\lambda_0^{-1}\pi^{-a}\pi^{b}\mu_0^{-1}\pi^{-b}\pi^{c+1}\nu_0^{-1}\pi^{-c-1}\sigma$$

Con incógnitas l y ρ.

Despejando $\pi^l\rho\pi^{-l}$, se obtiene que

$$\alpha^\tau = \pi^l\rho\pi^{-l}$$

Donde

$$\tau = \sigma\pi^{c+1}\nu\pi^{-c-1}\pi^{b}\mu\pi^{-b}\pi^{a}\lambda_0\pi^{-a}$$

Aplicando esto a los datos de un día se obtendra el cableado del reflector salvo conjugación, esto es, dicha permutación depende de la torsión del rotor de la izquierda, la cual aún no ha sido calculada.

Se toman, por ejemplo, los siguientes datos:

Orden Rotores	Ajuste Rotores	Ajuste Conjunto	Clavijero
I-IV-V	SPB TFG	(1,16,5)	(e n)(i g)(m a)(r w)(s k)(p b)

Cuya primera permutación es:

$$\alpha = (a\ y)(g\ u)(k\ l)(j\ w)(z\ f)(v\ c)(r\ o)(x\ n)(h\ d)(t\ p)(q\ s)(m\ b)(i\ e)$$

El primer paso es calcular τ.

$$\tau = \sigma\pi^{6}\nu\pi^{20}\pi^{16}\mu\pi^{10}\pi^{1}\lambda_0\pi^{25} = (a\ r\ k\ h\ s\ b\ l\ v\ f\ n\ e\ p\ u\ i\ m\ y\ x)(c\ z\ g\ t\ d\ j\ o)(q\ w)$$

Una vez obtenida τ, solo queda calcular ρ_0:

$$\rho_0 = \alpha^{\tau} = (r\ x)(t\ i)(h\ v)(o\ q)(g\ n)(f\ z)(k\ c)(a\ e)(s\ j)(d\ u)(w\ b)(y\ l)(m\ p)$$

Finalmente, la permutación que refleja el funcionamiento del reflector viene dada por:

$$\boxed{\rho = \pi^{-l}\rho_0\pi^{l}}$$

Por lo tanto, se ve claro que ρ es conocida salvo conjugación por π^l

3.6. Torsión rotor I y reflector

En este caso, el problema es encontrar un procedimiento apropiado para el calculo del valor de la torsión l que aparece en los apartados anteriores, 3.3.

En este trabajo se han utilizado como posiciones de los rotores en la máquina las dos siguientes: I-IV-V y I-V-IV, en ambas dos a la hora de sustituir en la ecuación modelo λ por $\lambda_0\pi^l$ y ρ por $\pi^{-l}\rho_0\pi^l$, desaparece el término π^n. Por lo tanto no es posible encontrar el valor de la torsión l usando solo la información de los dos meses de los que se dispone. Por la misma razón, tomando cualquier valor de l, se puede construir perfectamente una máquina Enigma que funcione pero solo si el orden de los rotores es uno de los dos anteriores.

En este apartado se va ha utilizar el mensaje cifrado que se utiliza como ejemplo en el libro de instrucciones de la máquina Enigma. De dicho ejemplo solo se va a utilizar la primera permutación que efectúa. Viene generado por la siguiente configuración:

Orden Rotores	Ajuste Rotores	Ajuste Conjunto	Clavijero
V-IV-I	PAT ROT	(2, 14, 0)	(k v)(o t)(h e)(p a)(r i)(c u)

Cuya clave del mensaje es: LIB.
Con esta configuración dada la primera permutación lleva la letra l a la letra j, es decir:

$$l\alpha_1 = j$$

Teniendo en cuenta el modelo matemático que refleja el funcionamiento de la máquina y los resultados ya obtenidos, se tiene:

$$\alpha = \sigma\pi\lambda_0\pi^{l}\pi^{13}\mu\ pi^{-12}\nu\pi^{-2}\pi^{-l}\rho_0\pi^{l}\pi^{2}\nu^{-1}\pi^{12}\mu^{-1}\pi^{-13}\pi^{-l}\lambda_0^{-1}\pi^{-1}\sigma$$

Como en esta ecuación solo es desconocido l, probando sus posibles valores se puede obtener la torsión buscada. En este caso $l = 4$

Lo que indica que el cabledo del rotor I y del reflector ρ son:

$$\boxed{\lambda = \lambda_0\pi^4 = (a\ e\ l\ t\ p\ h\ q\ x\ r\ u)(b\ k\ n\ w)(c\ m\ o\ y)(d\ f\ g)(i\ v)(j\ z)(s)}$$

$$\boxed{\rho = \pi^{-4}\rho_0\pi^4 = (a\ f)(b\ v)(c\ p)(d\ j)(e\ i)(g\ o)(h\ y)(k\ r)(l\ z)(m\ x)(n\ w)(q\ t)(s\ u)}$$

3.7. Turonver de los rotores

Para acabar de ver como funcionan los rotores de la máquina Enigma falta obtener el turnover de cada uno de los tres rotores utilizados. El turnover de un rotor se trata de cuando la muesca que esta situada en el anillo interior del rotor aparece en la ventanilla correspondiente y a la pulsación siguiente de cualquier letra el rotor situado a su izquierda gira $\frac{1}{26}$ de giro.

En sus trabajos [3] [4], Rejewski indicó que para encontrar dicha letra es suficiente con usar el ejemplo completo que aparece en el libro de instrucciones, el mismo ejemplo usado en el apartado anterior (este ejemplo consta, además de la configuración de la máquina, del texto plano y del texto cifrado). De hecho, solo son necesarias la configuración interna del rotor, la clave del mensaje y las primeras 26 letras de este ejemplo, ya que solo hay 26 posibles letras para ser el turnover del rotor. Se toma el mensaje cifrado a partir de la repetición de la clave del mensaje, es decir, solo se toma el mensaje enviado por eso se dice que solo se toma la configuración interna y la clave del mensaje.

Orden Rotores	Ajuste Rotores	Ajuste Conjunto	Clavijero
V-IV-I	PAT LIB	(8, 8, 22)	(k v)(o t)(h e)(p a)(r i)(c u)

Texto plano	mella mokvo thequ izash ayaso idoha blard emi
Texto cifrado	uaghd uryip uwbd jssoe ooqtt kspsv gjvsv ddb

Una vez recopilados los datos, se debe ir comprobando que la ecuación que modela a la máquina:

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

Al aplicarla a la letra en la posición i-ésima del texto plano da como resultado la letra situada en la posición i-ésima del texto cifrado. Se va comprobando las distintas posiciones posibles hasta que una de ellas no da la misma letra. Es decir, se comprueba que:

$$m\alpha_1 = u$$

En este caso, se produce una contradicción en la posición $i = 16$, ya que debería ser $i \to j$ pero se obtiene que:

$$i\alpha_{16} = p$$

Por lo tanto la letra del turnover será: 2(B)+16(i)-1= 17, es decir la letra Q.

Esta fórmula expresa la forma de obtener cuál es la letra del turnover. Se trata de la posición que ocupa la letra final de la clave del mensaje (aparece en la ventanilla), la letra B cuya posición en el abecedario es 2. 16(i) es la posición en la que las letras obtenidas mediante la fórmula no coinciden con las del mensaje. Por último se resta 1, ya que el turnover se produce en la siguiente pulsación de aparecer la letra en la ventanilla.

Para finalizar, falta obtener el turnover de los rotores restantes, IV y V. La forma de prodecer en este caso es distinta del método utilizado en el apartado anterior para obtener el turnover del rotor I, ya que en para estos casos no se tienen ejemplos completos, se tienen mensajes cifrados pero no con su correspondiente texto plano. Por ello el método cambia.

Gracias al trabajo efectuado anteriormente, se dispone de una completa descripción de la máquina mediante permutaciones salvo turnover, dada por :

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

La idea de calcular el turnover de los rotores es la siguiente: se trata de tomar uno de los mensajes interceptados a los alemanes al cual le corresponda una de las configuraciones incluidas en el libro de claves. Una vez seleccionado el mensaje, hay que ir descrifrandolo usando la fórmula que modela a Enigma. Llegará un momento en que el texto descifrado (texto plano) no tenga sentido. En ese momento se habrá producido el turnover.

Usando como orden de los rotores I-IV-V y I-V-IV, se obtendría el turnover de ambos rotores.

Para el caso con la siguiente configuración:

Orden Rotores	Ajuste Rotores	Ajuste Conjunto	Clavijero
I-V-IV	SAN PBA	(23, 1, 13)	(e n)(i g)(m a)(r w)(s k)(p b)

Mensaje cifrado:

JSQXX QTFCI EBUHI LYFZQ ...

Aplicando la ecuación con laa configuración dada, el texto plano sería:

ELEBR OGUAC Q ...

Se ve que a partir de la posición $i = 10$ el texto plano empieza a no tener sentido. Por lo tanto, la posición de la letra del turnocer es: 1(A)+10(i)-1= 10.

El turnover del rotor IV viene dado por la letra: J, ya que en el orden alfabetico *J* esta en la posición 10.

De forma análoga, con la configuración:

Orden Rotores	Ajuste Rotores	Ajuste Conjunto	Clavijero
I-IV-V	SPB TFG	(1, 16, 5)	(e n)(i g)(m a)(r w)(s k)(p b)

Se deduce que el turnover del rotor V viene dado por la letra: Z.

Bibliografía

[1] AUTORES CIENTÍFICO-TÉCNICOS Y ACADÉMICOS, *Criptografía y criptoanálisis en las dos guerras mundiales*, https://www.acta.es/medios/articulos/comunicacion_e_informacion/052063.pdf

[2] CIPHER MACHINES AND CRYPTOLOGY, http://users.telenet.be/d.rijmenants/en/enigmasim.htm

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

[4] M. REJEWSKI, *How Polish Mathematicians Deciphered the Enigma*, IEEE Annals of the History of Computing, Vol.3, No.3, July 1981

[5] M. VÁZQUEZ Y P. JIMÉNEZ, *Recovering the military Enigma using permitations- filling in the details of Rejewski's solution*,

[6] M. VÁZQUEZ Y P. JIMÉNEZ, *Teoría de permutaciones para ganar la segunda guerra mundial*