UNIVERSIDAD DE LA RIOJA

TRABAJO FIN DE ESTUDIOS

Título

Criptoanálisis de la máquina ENIGMA

Autor/es

DANIEL ARIAS RUIZ-ESQUIDE

Director/es

JOSÉ MARÍA PÉREZ IZQUIERDO

Facultad

Facultad de Ciencia y Tecnología

Titulación

Grado en Matemáticas

Departamento

MATEMÁTICAS Y COMPUTACIÓN

Curso académico

2017-18

publicaciones.unirioja.es
E-mail: publicaciones@unirioja.es

UNIVERSIDAD DE LA RIOJA

Facultad de Ciencia y Tecnología

TRABAJO FIN DE GRADO

Grado en Matemáticas

Criptoanálisis de la máquina ENIGMA

Cryptanalysis of the ENIGMA machine

Realizado por:

Daniel Arias Ruiz-Esquide

Tutelado por:

José María Pérez Izquierdo

Logroño, Junio 2018

Índice

1. Resumen

Este trabajo comienza con una recopilación de conceptos, resultados, métodos, herramientas y ejemplos que fueron utilizados para atacar a la máquina Engima.

El primero a tratar es el ataque polaco de Marian Rejewski. Este matemático, basándose en sus conocimientos de permutaciones, información fruto del espionaje y fallos de los operarios alemanes, consiguió el cableado de los rotores de la máquina sin haberlos visto, así como descrifrar los mensajes durante varios años.

Luego pasaremos al ataque con textos en claro de Alan Turing y su máquina, la Bomba. Necesaria para automatizar el de otra forma costoso proceso de conseguir las configuraciones de la Enigma para cada día ya que los alemanes corrigieron uno de sus grandes fallos, repetir la clave de sesión.

Finalmente dejamos los ataques históricos y nos centramos en conceptos estadísticos que pueden emplearse para realizar ataques solo con texto cifrado. Hacemos hincapié en la teoría de Claude Shannon pues estimó cuanto texto era necesario para conseguir la clave correcta.

2. Abstract

This document begins with a gathering of concepts, results, methods, tools and examples that were used to attack the Engima machine.

The first one to deal with is the Polish attack by Marian Rejewski. This mathematician, based on his knowledge of permutations, information resulting from espionage and failures of the German operators, got the wiring of the rotors of the machine without having even seen them, as well as deciphering the messages for several years.

Later we will move on to the attack with clear texts by Alan Turing and his machine, the Bomb. Necessary to automate the otherwise costly process of getting the Enigma settings for each day as the Germans corrected one of their major flaws, repeating the session key.

Finally we leave the historical attacks and focus on statistical concepts that can be used to perform attacks with encrypted text only. We emphasize the theory of Claude Shannon because he estimated how much text was necessary to get the correct key.

3. Introducción

Para situarnos vamos a dar unos matices sobre los orígenes y primeras muestras del uso de la criptografía y el criptoanálisis, seguido del contexto histórico de la máquina Enigma, la segunda guerra mundial, y una descripción de esta.

3.1. Breve historia de la criptografía y el criptoanálisis

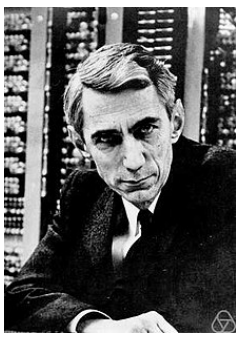
La criptografía o criptología ha estado presente desde el inicio de la comunicación, pues al crearse mensajes también se crea la necesidad de ocultarlos a los ojos de aquellos para los que no están destinados, nuestros enemigos.

La primera vez, de la que se tiene constancia, del uso de criptografía es en los jeroglíficos de Egipto. Mientras que muchos son claros de entender o esconden meros juegos hay otros que simplemente existen para complicar la lectura y dar a la historia más intriga.

Tras esto han ido surgiendo muchos cifrados diferentes, algunos ejemplos famosos son: el cifrado por números, *Atbash*, referenciado por Biblia; la escítala espartana, que servía para reordenar un mensaje escrito en una tira de pergamino; el cifrado César, usado por los romanos y que consistía en desplazar el abecedario una distancia fija; o el cifrado Vigenère, de Blaise de Vigenère, que consiste en tener una clave y aplicar varios cifrados César según la clave.

Al ser una pieza importantísisma de cualquier ejército, el ataque a los cifrados utilizados por los enemigos también se convirtió en ciencia, surge el criptoanálisis, que busca descifrar los mensajes encriptados. Personajes famosos de esta rama son Charles Babbage, que rompió el cifrado Vigenère con su Máquina Analítica; o Friedrich Kasiski, al que se le atribuyó el mérito de Babbage pues la investigación de este era secreta y Kasiski llegó al mismo resultado años más tarde. Un lingüista holandés, Auguste Kerckhoffs, también fue importante pues renovó la base de la criptografía postulando seis principios básicos que debía cumplir un sistema criptográfico o criptosistema para ser seguro. Este trabajo se centra en tres matemáticos y criptógrafos: Marian Rejewski, Alan Turing y Claude Shannon (de izquierda a derecha en las imágenes siguientes). Los dos primeros por atacar al cifrado de la máquina Enigma y el tercero por su trabajo en estadística para el criptoanálisis.





3.2. La guerra mundial y la máquina Enigma

Desde que las fuerzas militares alemanas adoptan la máquina Enigma en 1926 se convirtió en el método de encriptación principal utilizado por estas, extendiéndose su uso a la Segunda Guerra Mundial (1939-1945).

Esta utilización de la máquina se hubiera seguido dando de no ser por fallos de los operarios, expuestos más adelante; un gran trabajo del servicio de espionaje francés consiguiendo libros con claves de la máquina, como se puede ver en la siguiente imagen; e incluso que la Marina Real británica logró recuperar una máquina Enigma intacta de un submarino en 1942.

Geheim!

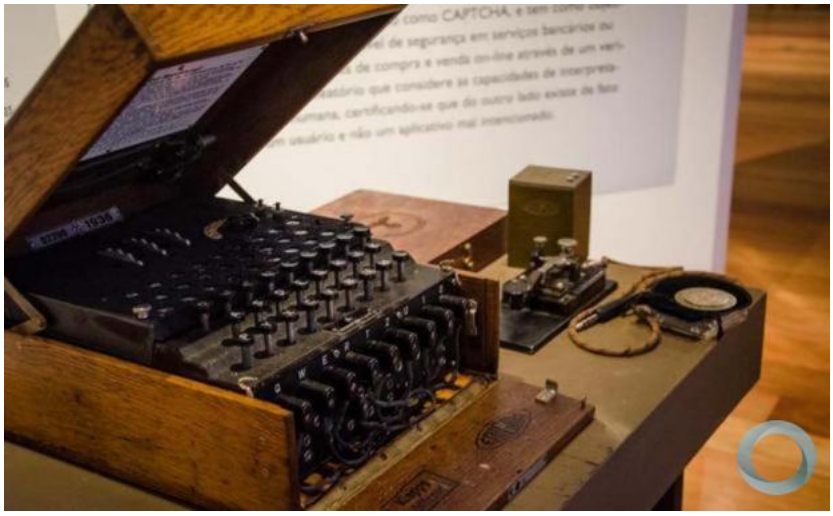
Sonder-Maschinenschlüssel BGT

Datum	Walzenlage	Ringstellung	Steckerverbindungen	Kenngruppe
31.	I V III	06 20 24	UA PF RQ BO NI EY BG HL TX ZJ	jeu nyq aqm
30.	V II III	01 07 12	GF KV JM FB UW LX TD QS NA ZH	azs zds kck
29.	IV I V	11 17 26	CI OK PV ZL HX NB AW DJ FE ST	kap gwh lyx

Pero sobre todo fue gracias al trabajo: en primer lugar de los polacos, que lograron superar la supuesta inviolabilidad de la máquina; y posteriormente los ingleses, instruidos por los polacos; que se logró descifrar los mensajes, llegando incluso a hacer cambiar su modo de uso a los alemanes; apoyándose en matemáticas y máquinas.

La máquina Enigma

El aparato del que vamos a hablar la mayoría del tiempo en este trabajo fue desarrollado en 1918 por la empresa Scherbius & Ritter. Se trata de una máquina eléctrica la cual podemos configurar de muchísimas formas posibles y una vez hecho encriptar un mensaje.

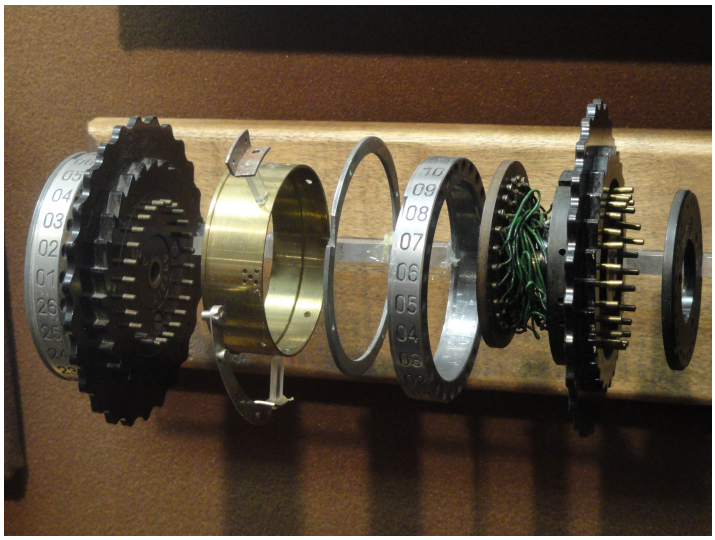


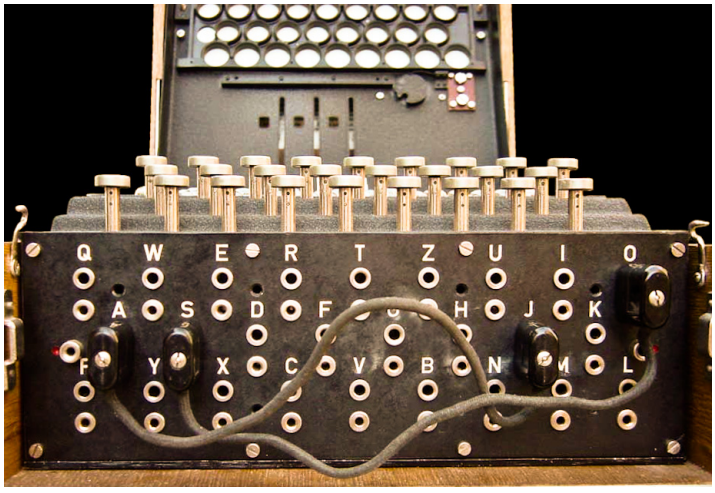
Hablaremos ahora de las partes que tenía la máquina:

- **Teclado:** la máquina presentaba un teclado QWERTZ de 26 letras. No había signos de puntuación, para representarlos se usaban combinaciones de letras.
- **Panel luminoso:** justo encima del teclado había una agrupación de 26 bombillas con las mismas 26 letras. El panel mostraba el resultado de la encriptación del carácter que pulsó el operario.
- **Rotor:** quizás la pieza clave a la hora de encriptar. Hubo varios modelos de rotores y de Enigmas según el número de los mismos. Estos eran cilindros con conexiones a ambos lados y cableado interno que unía las 26 conexiones de un lado con las del otro, haciendo una permutación en principio desconocida. Los rotores tenían nombres de números romanos: I, II, ... Poseían además un extremo a modo de rueda dentada, esto permitía el avance que luego explicaremos. Con el tiempo se desarrollaron rotores fijos. En su exterior tenían las 26 letras escritas en orden, o números que las representan, esto servía a la hora de configurar la máquina. Finalmente cada uno podía configurarse gracias a un anillo interno que servía para girar el cableado interno en relación al exterior del rotor.
- **Batería:** al ser una máquina eléctrica la necesitaba para funcionar, su capacidad era de unos $4,5$ voltios.
- **Reflector:** tras pasar por los rotores una vez, la señal se encontraba esta pieza. Se encarga de marcar la mitad del camino ya que la enviará otra vez por los mismos tres rotores. Las entradas, aunque también son salidas del reflector, están asociadas en parejas. Esto será útil más adelante pues significa que el reflector realiza una permutación que, descompuesta en ciclos, consta de trece 2-ciclos, estos corresponden a las trece parejas de entradas-salidas.
- **Tablero de conexiones:** situado debajo del teclado posee 26 clavijas, una para cada letra. En él se podían conectar cables uniendo dos de ellas, hacerlo significaba que pulsar una de las letras enviaba la señal de haber pulsado la otra a los rotores. Esto también se produce en la salida, si una letra está conectada con otra y la señal que sale de los rotores es la de una de las dos la señal que llegará al panel luminoso será la de la otra. Como podemos observar en la primera imagen de esta sección, la de un fragmento del libro capturado por el espionaje francés, se suelen utilizar 10 conexiones del tablero, cuarta columna del fragmento. Si calculamos cuantas posibilidades crea esta selección de 10 parejas de letras encontramos 150738274937250 distintas configuraciones. Este es uno de los hechos por los que Enigma era un sistema tan robusto e inexpugnable.

En la siguiente página encontramos, en orden, el teclado y panel luminoso, un rotor de la máquina y el tablero de conexiones.

Tras estas imágenes explicaremos cómo utilizaban la máquina los operarios alemanes y finalmente veremos un esquema de como viaja la señal por la máquina.




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

Cuando un operario debía cifrar un mensaje lo primero que hacía era configurar la máquina. Para ello leía en un libro común a todo el ejército cuál era la configuración para ese día. Incluía: qué rotores debía utilizarse, en qué orden, con qué configuración para su anillo y con qué clave del día, la cual era un conjunto de 3 letras a las que se establecían los rotores girándolos desde unas ventanas en la parte superior del panel luminoso. Puede apreciarse esto último en la foto del teclado anterior. Solo con los rotores no había terminado, debía también conectar los 10 cables del tablero de conexiones que indicaba el libro.

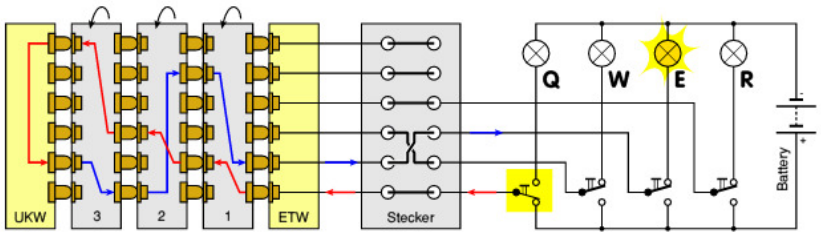
Entonces podía empezar a teclear, lo primero que debía escoger era una clave 3 letras llamada clave de sesión, para sí mismo, para ese momento en concreto y al decidirse la tecleaba en la máquina, dos veces. Tras hacerlo estos eran los 6 primeros caracteres del mensaje. Una vez escrita la clave de sesión sustituía a la del día en los rotores y con esta nueva configuración se tecleaba el mensaje oficial.

Así el destinatario solo tenía que descifrar los 6 primeros caracteres con la configuración del día para saber la clave de sesión utilizada y luego usar esta para desencriptar el mensaje.

Los principales errores de este sistema eran dos: los operarios podían elegir sus claves de sesión, esto llevaba a que por pereza o lo tedioso que era escribir con la Enigma las claves acababan siendo diagonales de teclado, tres letras repetidas o simples; y que la clave se repetía dos veces. Ahora veremos qué pasa a cada pulsación en la Enigma, pero como adelanto diremos que esto significa que la clave de sesión era cifrada con 2 claves diferentes.

Al pulsar una tecla en la Enigma lo primero que hace la máquina es el avance del rotor derecho, además si este está en una posición específica su movimiento arrastrará al central y si este también está en su posición especial arrastrará al izquierdo. Todo por como estaban diseñados los rotores. Una vez producido el avance, la señal viaja por las conexiones del tablero, luego por los rotores, llega al reflector, vuelve por los rotores en orden inverso y finalmente cruza una vez más el tablero para encender una bombilla del panel luminoso. El avance de los rotores esencialmente produce un cambio en la permutación que realiza la máquina a cada tecla pulsada. Esto parecía un gran obstáculo para los primeros que intentaron atacarla, pero para Rejewski fue lo que le permitió conseguirlo.

En la imagen hay una versión simplificada del circuito para 4 letras. Los rotores están marcados con números, UKW es el reflector, ETW es la entrada-salida a la zona de rotores, no realizaba una permutación; y el Stecker, de *Steckbrett*, es el tablero.



4. Teoría de permutaciones

4.1. Permutaciones

Cuando nos referimos a permutaciones pensamos inmediatamente en cambios, combinatoria. Si tenemos un conjunto con elementos, X, y cambiamos el orden de estos estamos efectuando una permutación.

Aclarar que vamos a trabajar sobre un conjunto de letras, el alfabeto, al cual consideramos $A = \{a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z\}$, sin la letra $\tilde{n}$. Para evitar confusiones usaremos la siguiente notación en las partes donde intervengan todas:

- Para conjuntos, letras mayúsculas A, B, C, D, ...
- Los elementos de los conjuntos serán números o minúsculas a, b, c, d, ...
- Y las permutaciones, letras caligráficas mayúsculas $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, $\mathcal{D}$, ...

Definición 1. *Sea X un conjunto no vacío a toda aplicación biyectiva $\mathcal{P}\colon X \to X$ se le denomina permutación de X.*

Definición 2. *Sean X un conjunto no vacío, $x, y \in X$ un par de elementos cualquiera y $\mathcal{P}$ una permutación de X. Si el resultado de aplicar $\mathcal{P}$ a x es y se dice que y es la imagen de x por $\mathcal{P}$ y se denota:*

$$x^{\mathcal{P}} = y$$

Una manera de representar una permutación es la notación en tabla o en dos líneas de Cauchy. Para ello se colocan todos los elementos del conjunto X en la primera línea y en la segunda sus imágenes al aplicar la permutación.

Ejemplo 1. *En este caso $\mathcal{P}$ será la permutación de elementos del conjunto $X = \{1, 2, 3\}$.*

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

Esta notación implica que $1^{\mathcal{P}} = 1$, $2^{\mathcal{P}} = 3$ y $3^{\mathcal{P}} = 2$.

Definición 3. *Sean X un conjunto no vacío y $\mathcal{P}$, $\mathcal{Q}$ permutaciones de X. A la acción de aplicar primero $\mathcal{P}$ y luego $\mathcal{Q}$ se le denomina composición, o producto, de permutaciones de X y seguimos la siguiente notación:*

Composición de $\mathcal{P}$ y $\mathcal{Q}$:

$$\mathcal{P}\mathcal{Q}$$

Imagen de $x \in X$ por $\mathcal{P}\mathcal{Q}$:

$$x^{\mathcal{P}\mathcal{Q}} = \left(x^{\mathcal{P}}\right)^{\mathcal{Q}}$$

La composición de permutaciones de X es otra permutación de X, esto es directo por la definición que hemos dado. La composición de aplicaciones biyectivas es biyectiva y el resultado es una aplicación de X a X luego una permutación de X. Para realizar la composición, teniendo ambas permutaciones en tabla, se reordena la segunda permutación de manera que su primera línea coincide con la segunda línea de la primera permutación, el resultado es la permutación que tiene la primera línea de la primera permutación y la segunda línea de la segunda permutación.

Ejemplo 2. *Sean $\mathcal{P}$ y $\mathcal{Q}$ las permutaciones de elementos del conjunto $X = \{1, 2, 3\}$ siguientes:*

$$\mathcal{P} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \mathcal{Q} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Su producto es

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

El mismo resultado puede conseguirse aplicando primero $\mathcal{P}$ y luego $\mathcal{Q}$:

$$1^{\mathcal{PQ}} = \left(1^{\mathcal{P}}\right)^{\mathcal{Q}} = 1^{\mathcal{Q}} = 3 \qquad 2^{\mathcal{PQ}} = \left(2^{\mathcal{P}}\right)^{\mathcal{Q}} = 3^{\mathcal{Q}} = 1 \qquad 3^{\mathcal{PQ}} = \left(3^{\mathcal{P}}\right)^{\mathcal{Q}} = 2^{\mathcal{Q}} = 2$$

Hay otro método, más tradicional, de componer permutaciones que se basa en hacer este cálculo al revés, es decir, de derecha a izquierda. Para mantener la notación usada en criptografía se ha optado por hacerlo así, de izquierda a derecha. Esta operación cumple las siguientes propiedades:

- **Asociativa:** sean $\mathcal{P}$, $\mathcal{Q}$ y $\mathcal{R}$ permutaciones de X: $\mathcal{P}(\mathcal{QR}) = (\mathcal{PQ})\mathcal{R}$
- **Permutación identidad:** sea X conjunto no vacío existe una permutación de X, $\mathcal{I}$, tal que $\forall x \in X$, $x^{\mathcal{I}} = x$.
- **Permutación inversa:** sea $\mathcal{P}$ permutación de X existe otra, $\mathcal{Q}$, tal que $\mathcal{PQ} = \mathcal{QP} = \mathcal{I}$. A esta $\mathcal{Q}$ se le denota $\mathcal{P}^{-1}$.

Definición 4. *Sean X un conjunto no vacío y $\mathcal{P}$ una permutación de X. Al mínimo entero n que hace $\mathcal{P}^n = \mathcal{I}$ con $\mathcal{I}$ la permutación identidad, se le denomina orden de $\mathcal{P}$.*

Así el conjunto de permutaciones de X es un grupo.

Definición 5. *Sea X un conjunto no vacío al grupo formado por las permutaciones de X con la composición como operación se le denomina grupo simétrico de X y su notación es S_X.*

Cuando X es un conjunto finito de n elementos nos referimos a su grupo simétrico como grupo simétrico de grado n, denotado por S_n. El cardinal de un grupo simétrico de grado n es $n!$

$$|S_n| = n!$$

Definición 6. *Sean X un conjunto no vacío, $x \in X$ un elemento de X y $\mathcal{P}$ una permutación de X. Si x es igual a su imagen por $\mathcal{P}$ se dice que x es un elemento fijo por $\mathcal{P}$.*

Ejemplo 3. *Retomemos $\mathcal{P}$ la permutación de elementos del conjunto $X = \{1, 2, 3\}$ que hemos usado anteriormente*

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

Podemos ver que 1 es fijo por $\mathcal{P}$ pues $1^{\mathcal{P}} = 1$.

Teorema 1. *(El grupo simétrico de orden mayor a 2 no es conmutativo) Sea X un conjunto finito de n elementos y S_n su grupo simétrico. Si $n \geq 3$ el grupo no es conmutativo.*

Definición 7. *Sean X un conjunto no vacío y $\mathcal{P}$ una permutación de X. Al conjunto de elementos de X que no son fijos por $\mathcal{P}$ se le donomina soporte de $\mathcal{P}$ y se denota $X_{\mathcal{P}}$*

Definición 8. *Sean X un conjunto no vacío y $\mathcal{P}$, $\mathcal{Q}$ permutaciones de X. Si se cumple que*

$$X_{\mathcal{P}} \cap X_{\mathcal{Q}} = \emptyset$$

se dice que $\mathcal{P}$ y $\mathcal{Q}$ son permutaciones disjuntas.

Ejemplo 4. *Sean $\mathcal{P}$ y $\mathcal{Q}$ las permutaciones de elementos del conjunto $X = \{1, 2, 3\}$ usadas anteriormente podemos hallar sus soportes viendo que en $\mathcal{P}$ solo es fijo el 1 y en $\mathcal{Q}$ solo es fijo el 2.*

$$X_{\mathcal{P}} = \{2, 3\}, \quad X_{\mathcal{P}} = \{1, 3\}, \quad X_{\mathcal{P}} \cap X_{\mathcal{Q}} = \{3\} \neq \emptyset$$

Así $\mathcal{P}$ y $\mathcal{Q}$ no son disjuntas pues la intersección de sus soportes no es el conjunto vacío.

Un resultado interesante de esta parte es que el producto de permutaciones no tiene por qué ser conmutativo. No obstante, al tener en cuenta si dos permutaciones son disjuntas surge el siguiente teorema.

Teorema 2. *(Las permutaciones disjuntas conmutan) Sean X un conjunto no vacío y $\mathcal{P}$,$\mathcal{Q}$ permutaciones de X. Si $\mathcal{P}$ y $\mathcal{Q}$ son disjuntas conmutan;*

$$X_{\mathcal{P}} \cap X_{\mathcal{Q}} = \emptyset \Rightarrow \mathcal{P}\mathcal{Q} = \mathcal{Q}\mathcal{P}$$

Las permutaciones pueden descomponerse en otras estructuras algebraicas más simples, estos son los llamados ciclos de los que daremos definiciones y resultados a continuación.

4.2. Ciclos

Un caso especial de permutación que fija algunos elementos del conjunto y mueve cíclicamente el resto es el concepto que entendemos por ciclo.

Definición 9. *Sean $X = \{1, 2, \ldots, n\}$ un conjunto finito de n elementos y $\mathcal{P}$ una permutación de X y por lo tanto $\mathcal{P} \in S_n$. Si $\mathcal{P}$ cumple que existe $I = \{x_1, x_2, \ldots, x_m\} \subseteq X$, con $x_i \in X$, para todo $i \in [1, m]$, tal que:*

- $\forall x \in X,\ x \notin I,\ x^{\mathcal{P}} = x$
- ${x_i}^{\mathcal{P}} = x_{i+1},\ \forall i \in [1, m-1]$
- ${x_m}^{\mathcal{P}} = x_1$

Entonces se dirá que $\mathcal{P}$ es un ciclo y será representado como $(x_1\, x_2\, \ldots\, x_m)$.

Definición 10. *Sean $X = \{1, 2, \ldots, n\}$ un conjunto finito de n elementos y $\mathcal{C} = (x_1\, x_2\, \ldots\, x_m)$, con $x_i \in X$, para todo $i \in [1, m]$, un ciclo. Se dice que el ciclo es de longitud m. Se denota $o(\mathcal{C}) = m$ y se dice que $\mathcal{C}$ es un m-ciclo.*

Nota 1. *En ciclos los conceptos de orden y longitud son el mismo. Resultado obtenido directamente de la definición de ciclo.*

El siguiente teorema nos ayuda a descomponer una permutación en un producto de ciclos disjuntos.

Teorema 3. *Toda permutación $\mathcal{P} \in S_n$, distinta de la permutación identidad, $\mathcal{I}$, puede expresarse como producto de ciclos disjuntos con longitudes mayores o iguales a 2. Esta descomposición es única salvo en el orden de los factores.*

Demostración. Primero demostraremos la existencia y luego la unicidad de esta descomposición.

Sea $\mathcal{P}$ una permutación cualquiera de S_n

$$\mathcal{P} = \begin{pmatrix} 1 & 2 & \ldots & n \\ p_1 & p_2 & \ldots & p_n \end{pmatrix}$$

Pueden darse dos casos:

1. $\mathcal{P} = \mathcal{I}$ al ser la identidad deja todo fijo, no hay ciclos.
2. $\mathcal{P} \neq \mathcal{I}$ el caso que asumiremos.

Tomamos un número $x \in [1, n]$ no fijo, es decir, $i^{\mathcal{P}} \neq i$. Con este vamos construyendo $x^{\mathcal{P}}$, $x^{\mathcal{P}^2}, \ldots,$ $x^{\mathcal{P}^m}$, parando cuando $x^{\mathcal{P}^{m+1}} = x$. Con estos elementos tenemos el m-ciclo $(x\, x^{\mathcal{P}}\, x^{\mathcal{P}^2} \ldots\, x^{\mathcal{P}^m})$ que constituye parte de (o toda) la permutación $\mathcal{P}$. Estamos, de nuevo, ante dos situaciones.

1. $\mathcal{P}$ no contiene más números que podamos tomar como x. Es decir no quedan números que no sean fijos y que no estén ya en un ciclo.
2. $\mathcal{P}$ los contiene. Repetiremos la construcción de un nuevo ciclo para otro de estos números. Sucesivamente, al ser una permutación de un grupo simétrico finito, llegaremos a una descomposición en ciclos.

Entonces existen las descomposiciones en ciclos disjuntos. Según el orden en el que los vamos construyendo los vamos numerando con subíndices y al final la permutación $\mathcal{P}$ puede expresarse como:

$$\mathcal{P} = \mathcal{P}_1\mathcal{P}_2 \dots \mathcal{P}_r \quad r \in \mathbb{N}$$

Nota 2. *Recordamos que las permutaciones, y en particular los ciclos, son biyecciones. Entonces no puede darse que, contruyendo un nuevo ciclo, nos aparezca un término que ya está en uno de los construidos. Es decir, si contruyendo $\mathcal{P}_i$ nos aparece un término que está en $\mathcal{P}_j$ con $j<i$, significa que dicho término tiene dos preimágenes por $\mathcal{P}$ y entonces esta no es biyectiva.*

Ahora veamos que es única.

Asumimos que $\mathcal{P}$ admite dos descomposiciones distintas:

$$\begin{cases} \mathcal{P} = \mathcal{P}_1\mathcal{P}_2 \dots \mathcal{P}_r \\ \mathcal{P} = \mathcal{P}'_1\mathcal{P}'_2 \dots \mathcal{P}'_s \end{cases}$$

Si tomamos un número x_1, no fijo por $\mathcal{P}$, estará en uno, y solo uno, de los ciclos de cada descomposición. Ya que estos ciclos conmutan por ser disjuntos asumimos que son $\mathcal{P}_1$ y $\mathcal{P}'_1$. Sabemos que x_1 es fijo por el resto de los ciclos de ambas descomposiciones y que $x_2 = {x_1}^{\mathcal{P}}$ es único. Estos mismos argumentos se repiten con x_2 y sucesivamente llegamos a que $\mathcal{P}_1 = \mathcal{P}'_1$.

Repitiendo todo el procedimiento llegamos a que $r = s$ y $\mathcal{P}_i = \mathcal{P}'_i$ $\forall i \in [1, r]$ Por lo tanto, la descomposición es única. □

Si nos encontramos ante una permutación descompuesta en ciclos no disjuntos podemos encontrar su descomposicón única de una forma similar. Escogemos un elemento del conjunto en el que se haga la permutación y le aplicamos los ciclos no disjuntos, con esto conseguimos su imagen por la permutación, repetimos el proceso con la imagen hasta volver al primer elemento. Luego repetimos si no hemos agotado todos los elementos no fijos por la permutación.

Nota 3. *Propiedades relacionadas con las inversas, son directas de la definición de ciclo.*

- *Sea $\mathcal{C} = (c_1\, c_2\, \dots\, c_n)$ un ciclo. Su inverso, $\mathcal{C}^{-1} = (c_n\, c_{n-1}\, \dots\, c_1)$, también lo es.*
- *Si tenemos una permutación descompuesta en r ciclos disjuntos $\mathcal{P} = \mathcal{P}_1\mathcal{P}_2 \dots \mathcal{P}_r$. Su inversa es $\mathcal{P}^{-1} = {\mathcal{P}_1}^{-1}{\mathcal{P}_2}^{-1} \dots {\mathcal{P}_r}^{-1}$*

Proposición 1. *Sea la permutación $\mathcal{P} \in S_n$ y $\mathcal{P}_1\mathcal{P}_2 \dots \mathcal{P}_r$ su descomposición en ciclos disjuntos. Se tiene que su orden es el mínimo común múltiplo de los ordenes de los ciclos disjuntos.*

$$o(\mathcal{P}) = \text{mcm}(o(\mathcal{P}_1), o(\mathcal{P}_2), \dots, o(\mathcal{P}_r))$$

4.3. Transposiciones

Definición 11. *Sea $\mathcal{C}$ un 2-ciclo, se dice que $\mathcal{C}$ es una transposición. En otras palabras, los ciclos de longitud u orden 2 se denominan transposiciones.*

Teorema 4. *Cualquier permutación $\mathcal{P}$, puede expresarse como producto de transposiciones. Esta descomposición no tiene por qué ser única.*

Demostración. Nos basta probar que todo ciclo, $\mathcal{C}$, puede descomponerse en transposiciones, o 2-ciclos. Como no tiene que ser única simplemente podemos elegir

$$\mathcal{C} = (c_1\, c_2\, \dots\, c_n) = (c_1\, c_2)(c_1\, c_3) \dots (c_1\, c_n)$$

y ya tenemos una descomposición en transposiciones. □

Al ver la descomposción podríamos intentar descubrir si es única. Esto no es cierto. Sin embargo, sí se puede demostrar que la paridad del número de transposiciones en las que se descompone un permutación no varía.

Definición 12. *Sea $\mathcal{P}$ una permutación, si se puede descomponer en un número par de transposiciones se denomina permutación par. De lo contrario, puede descomponerse en un número impar de transposiciones, se denomina permutación impar.*

Teorema 5. *Sea $\mathcal{P}$ una permutación tal que $\mathcal{P} = \mathcal{P}_1\mathcal{P}_2 \dots \mathcal{P}_r = \mathcal{P}'_1\mathcal{P}'_2 \dots \mathcal{P}'_s$ sean dos descomposiciones en transposiciones posibles para $\mathcal{P}$. Entonces r y s tienen la misma paridad. Dicho de otra manera $\mathcal{P}$ no puede ser par e impar a la vez.*

4.4. Conjugación

Definición 13. *Sean $\mathcal{P}$, $\mathcal{Q} \in S_n$ dos permutaciones. Si existe otra permutación $\mathcal{R} \in S_n$ tal que $\mathcal{Q} = \mathcal{R}\mathcal{P}\mathcal{R}^{-1}$ se dice que $\mathcal{P}$ y $\mathcal{Q}$ son conjugadas o semejantes.*

Definición 14. *Sean $\mathcal{P}$, $\mathcal{Q} \in S_n$ dos permutaciones. Si para todo $m \in \mathbb{N}$ el número de m-ciclos en $\mathcal{P}$ es igual al número de m- ciclos en $\mathcal{Q}$ se dice que $\mathcal{P}$ y $\mathcal{Q}$ tienen la misma estructura en ciclos. Obviamente, es necesario conocer las descomposiciones únicas en ciclos de $\mathcal{P}$ y $\mathcal{Q}$.*

Teorema 6. *Sean $\mathcal{P}$, $\mathcal{Q} \in S_n$ dos permutaciones. Se tiene que $\mathcal{P}$ y $\mathcal{Q}$ son conjugadas si y solo si $\mathcal{P}$ y $\mathcal{Q}$ tienen la misma estructura en ciclos*

Este resultado puede ser utilizado para determinar todas las posibles $\mathcal{R}$ que hacen semejantes a dos permutaciones $\mathcal{P}$ y $\mathcal{Q}$.

Para ello descomponemos ambas en ciclos y al tener la misma estructura podemos agrupar ciclos de longitud r de $\mathcal{P}$ con los de la misma longitud de $\mathcal{Q}$. Colocamos los ciclos en dos líneas. En la primera el r-ciclo de $\mathcal{P}$ y en la segunda un r-ciclo de $\mathcal{Q}$. Este último en cualquier ordenación, sin que deje de ser el mismo ciclo.

La permutación formada por los pares verticales es una $\mathcal{R}$ de las múltiples que hace $\mathcal{P}$ y $\mathcal{Q}$ semejantes. El total de posibilidades depende de cuantas formas puedan agruparse los r-ciclos y de cuantas maneras pueden ordenarse los elementos dentro de los de $\mathcal{Q}$.

5. El ataque polaco

Marian Rejewski modeló la máquina Enigma como un producto de permutaciones y con ayuda del espionaje francés que consiguió un libro con el orden de los rotores, las conexiones del panel y la configuración incial de la máquina. Rejewski utilizó esto para recrear las permutaciones de los rotores sin haber tenido nunca uno en las manos. Hizo el siguiente planteamiento.

5.1. Planteamiento

La máquina Enigma es un producto de permutaciones y por lo tanto una permutación. La permutación que realiza la máquina es:

$$Enigma \equiv \mathcal{S}\mathcal{N}\mathcal{M}\mathcal{L}\mathcal{R}\mathcal{L}^{-1}\mathcal{M}^{-1}\mathcal{N}^{-1}\mathcal{S}^{-1}$$

Siendo $\mathcal{N}$ el rotor derecho, $\mathcal{M}$ el rotor central, $\mathcal{L}$ el izquierdo y $\mathcal{R}$ el reflector. Podríamos considerar el giro del anillo de los rotores, pero esto no cambia el cableado interno así que por comodidad no se tendrá en cuenta. La permutación $\mathcal{S}$ es el panel de conexiones. No obstante, esta permutación era conocida así que por simplificar las cosas la obviaremos quedando:

$$Enigma \equiv \mathcal{N}\mathcal{M}\mathcal{L}\mathcal{R}\mathcal{L}^{-1}\mathcal{M}^{-1}\mathcal{N}^{-1}$$

Pero la máquina cambia su permutación con cada tecla que pulsamos, por ello consideramos la permutación tras pulsar la i-ésima tecla:

$$Enigma_i \equiv \mathcal{N}_i\mathcal{M}_i\mathcal{L}_i\mathcal{R}\mathcal{L}'_i\mathcal{M}'_i\mathcal{N}'_i \tag{1}$$

Aquí es importante decir que $\mathcal{N}_i$ es $\mathcal{P}^i\mathcal{N}\mathcal{P}^{-i}$ y $\mathcal{N}'_i$ es $\mathcal{P}^i\mathcal{N}^{-1}\mathcal{P}^{-i}$ con $\mathcal{P}$ la permutación que a cada letra le asigna la siguiente, es decir, que descompuesta en ciclos es el 26-ciclo:

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

Con esta definición $\mathcal{N}_i'$ es la inversa de $\mathcal{N}_i$. Análogo para $\mathcal{M}_i$, $\mathcal{M}_i'$, $\mathcal{L}_i$ y $\mathcal{L}_i'$.

Como siguiente paso se fijó en que los mensaje comenzaban con una clave de sesión de 3 letras escrita 2 veces, es decir 6 letras tales que, descifradas, la primera era igual a la cuarta, la segunda a la quinta y la tercera a la sexta.

Rejewski consideró seis permutaciones $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, $\mathcal{D}$, $\mathcal{E}$ y $\mathcal{F}$, de modo que $\mathcal{A} \equiv Enigma_1$ es la permutación para la primera tecla pulsada, $\mathcal{B} \equiv Enigma_2$ es para la segunda y análogo para el resto.

Podemos ver que estas permutaciones son conjugadas del rotor de la máquina, $\mathcal{R}$.

Ejemplo 5. *En el caso de $\mathcal{A}$, la hemos definido como $Enigma_1$, es decir,*

$$\mathcal{A} = \mathcal{N}_1\mathcal{M}_1\mathcal{L}_1\mathcal{R}\mathcal{L}_1'\mathcal{M}_1'\mathcal{N}_1'$$

tomamos $\mathcal{N}_1\mathcal{M}_1\mathcal{L}_1$ como una permutación $\mathcal{H}$ y notamos que $\mathcal{H}^{-1} = \mathcal{L}_1'\mathcal{M}_1'\mathcal{N}_1'$, dejando

$$\mathcal{A} = \mathcal{H}\mathcal{R}\mathcal{H}^{-1}$$

y aquí vemos claro que son conjugadas. El proceso es el mismo para el resto.

Aplicando el teorema 6 el hecho de que sean conjugadas significa que tienen la misma estructura en ciclos, es decir, que las permutaciones $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, $\mathcal{D}$, $\mathcal{E}$ y $\mathcal{F}$ constan de trece 2-ciclos disjuntos. Esto también significa que las seis permutaciones son iguales a sus inversas.

A continuación propuso tres permutaciones más que relacionarían las letras iguales de la clave de sesión. Supongamos que la clave de sesión de tres letras es $c_1c_2c_3$, una vez cifrada aparecería como $x_1x_2x_3x_4x_5x_6$, sabemos que x_1 y x_4 son las imágenes de misma letra, c_1, pero cifrada por diferentes permutaciones:

$$c_1{}^{\mathcal{A}} = x_1 \qquad c_1{}^{\mathcal{D}} = x_4$$

Considerando que las permutaciones $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, $\mathcal{D}$, $\mathcal{E}$ y $\mathcal{F}$ deben ser iguales a sus inversas tenemos que:

$$x_1{}^{\mathcal{A}} = x_1{}^{\mathcal{A}^{-1}} = c_1 \qquad x_4{}^{\mathcal{D}} = x_4{}^{\mathcal{D}^{-1}} = c_1$$

Usando la permutación que llamaremos $\mathcal{A}\mathcal{D}$, y que es el producto de $\mathcal{A}$ y $\mathcal{D}$, puede conseguirse pasar de x_1 a x_4:

$$x_1{}^{\mathcal{A}\mathcal{D}} = (x_1^{\mathcal{A}})^{\mathcal{D}} = c_1{}^{\mathcal{D}} = x_4$$

Con este mismo planteamiento se crean las permutaciones $\mathcal{B}\mathcal{E}$ para pasar de x_2 a x_5 y $\mathcal{C}\mathcal{F}$ para pasar de x_3 a x_6.

Con muchos mensajes cifrados las tablas de $\mathcal{A}\mathcal{D}$, $\mathcal{B}\mathcal{E}$ y $\mathcal{C}\mathcal{F}$ podían calcularse, pero para conseguir información sobre el primer rotor había que extraer las permutaciones $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, $\mathcal{D}$, $\mathcal{E}$ y $\mathcal{F}$. Rejewski propuso y demostró un teorema que servía para esto.

Teorema 7. *Si dos permutaciones, sobre el mismo conjunto, que tienen la misma estructura en ciclos solo poseen transposiciones disjuntas en su descomposición. Entonces su producto consistirá en una o varias parejas de ciclos de la misma longitud.*

Demostración. Sean dos permutaciones $\mathcal{X}$ e $\mathcal{Y}$ sobre un conjunto finito de $2n$ elementos, luego $\mathcal{X}, \mathcal{Y} \in S_{2n}$. Suponemos que $\mathcal{X}$ e $\mathcal{Y}$ tienen la propiedad del enunciado.

Si al descomponerse en ciclos encontramos $(a_1\, a_2)$ en $\mathcal{X}$ y el mismo en $\mathcal{Y}$ entonces su producto tendrá $(a_1)(a_2)$ entre otros ciclos, es decir, encontramos dos 1-ciclos, una pareja.

Ahora generalizamos esto diciendo que en su descomposición encontramos transposiciones que podemos ir encadenando, una en $\mathcal{X}$, otra en $\mathcal{Y}$ y repetimos hasta un término a_{2k} pues volvemos a a_1, es decir, $a_{2k}^{\mathcal{Y}} = a_1$.

- En la de $\mathcal{X}$ encontramos $(a_1\, a_2)(a_3\, a_4)\ldots(a_{2k-3}\, a_{2k-2})(a_{2k-1}\, a_{2k})$.
- En la de $\mathcal{Y}$ encontramos $(a_2\, a_3)(a_4\, a_5)\ldots(a_{2k-2}\, a_{2k-1})(a_{2k}\, a_1)$.

En el producto $\mathcal{X}\mathcal{Y}$ encontraremos

$$(a_1\, a_3\, \ldots\, a_{2k-3}\, a_{2k-1})(a_{2k}\, a_{2k-2}\, \ldots\, a_4\, a_2)$$

entre otros ciclos, es decir, encontramos una pareja de k-ciclos.

Como k puede ser igual o menor a n podemos haber acabado con esta pareja, si k es igual a n, o no, si es menor. Si no se cubren todos los elementos, basta repetir el proceso con los restantes. Las longitudes de todos los ciclos sumarán $2n$ cuando hayamos acabado. □

Al ser las permutaciones $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, $\mathcal{D}$, $\mathcal{E}$ y $\mathcal{F}$ válidas para usar este teorema, Rejewski comprobó satisfecho que las permutaciones que conocían, $\mathcal{AD}$, $\mathcal{BE}$ y $\mathcal{CF}$, cumplían el resultado, tenían parejas de ciclos de la misma longitud. Ahora hacía falta un método para conseguir las otras. Desarrollaremos el proceso a modo de ejemplo para las permutaciones $\mathcal{A}$, $\mathcal{D}$ y $\mathcal{AD}$ pero es el mismo para $\mathcal{B}$, $\mathcal{E}$, $\mathcal{BE}$, $\mathcal{C}$, $\mathcal{F}$ y $\mathcal{CF}$.

Ejemplo 6. *Según el teorema 7 si dos elementos a_1 y b_1 forman una transposición de $\mathcal{A}$, $(a_1\, b_1)$, es de esperar que se encuentren en dos ciclos distintos de $\mathcal{AD}$, pero sabemos que estos tienen la misma longitud. Cogemos entonces dos ciclos de $\mathcal{AD}$ de la misma longitud, uno que tenga a a_1 y el otro a b_1, $(a_1\, a_2\, \ldots\, a_{r-1}\, a_r)$ y $(b_r\, b_{r-1}\, \ldots\, b_2\, b_1)$.*

Es importante fijarse que el segundo aparecerá en $\mathcal{AD}$ de manera inversa, esto se puede ver en la demostración del teorema. Quizás b_1 no es el último del ciclo, pero puede reordenarse para que lo sea. Entonces escribimos los ciclos uno encima del otro, tomando ahora el segundo

ya ordenado:

$$(a_1\, a_2\, \ldots\, a_{r-1}\, a_r)$$
$$(b_1\, b_2\, \ldots\, b_{r-1}\, b_r)$$

Si sabíamos que $(a_1\, b_1)$ *era una transposición de las de* $\mathcal{A}$ *podemos tomar como los pares verticales, es decir,* $(a_1\, b_1)(a_2\, b_2)\ldots(a_r\, b_r)$.

Para obtener $\mathcal{D}$ *tendríamos que conocer una de sus transposiciones y hacer el mismo proceso.*

Si no conocemos ninguna transposición podremos conseguir todas las posibles $\mathcal{A}$, *o* $\mathcal{D}$, *agrupando parejas de ciclos de* $\mathcal{AD}$ *con la misma longitud, el segundo de manera inversa a como aparece en* $\mathcal{AD}$, *y usando todas las reordenaciones posibles del segundo. Esto significa que en el mejor caso, que* $\mathcal{AD}$ *tenga dos* 13*-ciclos, tenemos 13 posibilidades para* $\mathcal{A}$. *El número de transposiciones que tenemos que conocer es el número de parejas de ciclos de igual longitud que hay en* $\mathcal{AD}$ *menos uno.*

Sin embargo, gracias al espionaje francés y los fallos de los escritores alemanes se tenían algunas transposiciones de las permutaciones o se podían deducir.

Una vez conocidas $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, $\mathcal{D}$, $\mathcal{E}$ y $\mathcal{F}$, el siguiente paso era utilizarlas para conocer los rotores, pero el cómo hacerlo era la parte complicada. Hacer cálculos con los tres rotores algo costoso por el número de incógnitas así que Rejewski se centró en el primer rotor, el derecho, en el caso de que solo se moviera este y ninguno más.

Nota 4. *Ya que solo una posición obliga al avance del siguiente rotor pensemos que es la posición* i *en el caso del rotor derecho, con* $i \in [0, 25]$. *Consideremos las posiciones en módulo 26. Al pulsar una tecla lo primero que hace la máquina es avanzar el rotor derecho una posición y si pasa de la posición* i *a* $i+1$ *hará avanzar una al rotor central, este es el caso que queremos evitar. Configurar entonces la máquina en las posiciones* i, $i-1$, $i-2$, $i-3$, $i-4$ *o* $i-5$ *hará que se mueva el rotor central en alguna de las 6 pulsaciones. Si quitamos estas 6 posiciones nos quedan 20 en las que solo avanza el derecho. Sabiendo esto, el caso que aisló Rejewski ocurría el* $76,92\,\%$ *de las veces.*

Aceptando esta consideración, en la fórmula de $Enigma_i$ (Ecuación 1) podemos sustituir $\mathcal{M}_i\mathcal{L}_i\mathcal{R}\mathcal{L}_i'\mathcal{M}_i'$ por $\mathcal{Q}$ una permutación que no va a depender de que número de pulsaciones hayamos realizado, pues como hemos dicho ni el rotor central, $\mathcal{M}$, ni el izquierdo, $\mathcal{L}$, van a moverse. La fórmula queda:

$$Enigma_i \equiv \mathcal{P}^i\mathcal{N}\mathcal{P}^{-i}\mathcal{Q}\mathcal{P}^i\mathcal{N}^{-1}\mathcal{P}^{-i}$$
$$Enigma_i \equiv \mathcal{N}_i\mathcal{Q}\mathcal{N}_i'$$

Ahora pensamos como utilizar esto para obtener $\mathcal{N}$. Hay que buscar la manera de simplificar el sistema. Rejewski introdujo las expresiones que vemos a continuación.

$$\mathcal{U} = \mathcal{N}\mathcal{P}^{-1}\mathcal{Q}\mathcal{P}\mathcal{N}^{-1}$$
$$\mathcal{V} = \mathcal{N}\mathcal{P}^{-2}\mathcal{Q}\mathcal{P}^{2}\mathcal{N}^{-1}$$
$$\mathcal{W} = \mathcal{N}\mathcal{P}^{-3}\mathcal{Q}\mathcal{P}^{3}\mathcal{N}^{-1}$$
$$\mathcal{X} = \mathcal{N}\mathcal{P}^{-4}\mathcal{Q}\mathcal{P}^{4}\mathcal{N}^{-1}$$
$$\mathcal{Y} = \mathcal{N}\mathcal{P}^{-5}\mathcal{Q}\mathcal{P}^{5}\mathcal{N}^{-1}$$
$$\mathcal{Z} = \mathcal{N}\mathcal{P}^{-6}\mathcal{Q}\mathcal{P}^{6}\mathcal{N}^{-1}$$
$$\mathcal{J} = \mathcal{N}\mathcal{P}\mathcal{N}^{-1}$$

Una vez más, despejaremos para $Enigma_1$, la que denominamos $\mathcal{A}$. Para el resto, $\mathcal{B}$, $\mathcal{C}$, $\mathcal{D}$, $\mathcal{E}$ y $\mathcal{F}$; es el mismo procedimiento.

Tenemos la siguiente permutación,

$$\mathcal{A} = \mathcal{N}_1\mathcal{Q}\mathcal{N}_1'$$

y utilizamos que $\mathcal{N}_i$ es $\mathcal{P}^i\mathcal{N}\mathcal{P}^{-i}$ y $\mathcal{N}_i'$ es $\mathcal{P}^i\mathcal{N}^{-1}\mathcal{P}^{-i}$, lo que nos deja,

$$\mathcal{A} = \mathcal{P}\mathcal{N}\mathcal{P}^{-1}\mathcal{Q}\mathcal{P}\mathcal{N}^{-1}\mathcal{P}^{-1}$$

Haciendo algunas transformaciones llegamos a

$$\mathcal{P}^{-1}\mathcal{A}\mathcal{P} = \mathcal{N}\mathcal{P}^{-1}\mathcal{Q}\mathcal{P}\mathcal{N}^{-1} = \mathcal{U}$$

Y como ya hemos adelantado trabajando con $\mathcal{B}$, $\mathcal{C}$, $\mathcal{D}$, $\mathcal{E}$ o $\mathcal{F}$, llegaríamos a $\mathcal{V}$, $\mathcal{W}$, $\mathcal{X}$, $\mathcal{Y}$ o $\mathcal{Z}$ respectivamente. Podemos ver entonces que conocidas las seis primeras las nuevas expresiones introducidas por Rejewski son simplemente una conjugación por $\mathcal{P}$.

Las propuso porque al trabajar con las permutaciones compuestas $\mathcal{U}\mathcal{V}$, $\mathcal{V}\mathcal{W}$, $\mathcal{W}\mathcal{X}$, $\mathcal{X}\mathcal{Y}$ e $\mathcal{Y}\mathcal{Z}$ nos damos cuenta de que son semejantes entre sí, si aplicamos la última expresión, $\mathcal{J}$. Y si descubrimos $\mathcal{J}$ podemos descubrir las posibles $\mathcal{N}$, ya que esta última es la permutación que se usa para hacer semejantes a $\mathcal{J}$ y $\mathcal{P}$.

Veamos de dónde sale este $\mathcal{J}$. Empezaremos viendo como es $\mathcal{U}\mathcal{V}$:

$$\mathcal{U} = \mathcal{P}^{-1}\mathcal{A}\mathcal{P}$$
$$\mathcal{V} = \mathcal{P}^{-2}\mathcal{B}\mathcal{P}^{2}$$
$$\mathcal{U}\mathcal{V} = \mathcal{P}^{-1}\mathcal{A}\mathcal{P}\mathcal{P}^{-2}\mathcal{B}\mathcal{P}^{2} = \mathcal{P}^{-1}\mathcal{A}\mathcal{P}^{-1}\mathcal{B}\mathcal{P}^{2}$$

Utilizamos las expresiones de $\mathcal{A}$ y $\mathcal{B}$:

$$\begin{aligned}
\mathcal{UV} &= \mathcal{P}^{-1}\mathcal{P}\mathcal{N}\mathcal{P}^{-1}\mathcal{Q}\mathcal{P}\mathcal{N}^{-1}\mathcal{P}^{-1}\mathcal{P}^{-1}\mathcal{P}^{2}\mathcal{N}\mathcal{P}^{-2}\mathcal{Q}\mathcal{P}^{2}\mathcal{N}^{-1}\mathcal{P}^{-2}\mathcal{P}^{2} \\
\mathcal{UV} &= \mathcal{N}\mathcal{P}^{-1}\mathcal{Q}\mathcal{P}\mathcal{N}^{-1}\mathcal{P}^{-2}\mathcal{P}^{2}\mathcal{N}\mathcal{P}^{-2}\mathcal{Q}\mathcal{P}^{2}\mathcal{N}^{-1} \\
\mathcal{UV} &= \mathcal{N}\mathcal{P}^{-1}\mathcal{Q}\mathcal{P}^{-1}\mathcal{Q}\mathcal{P}^{2}\mathcal{N}^{-1} \\
\mathcal{UV} &= \mathcal{N}\mathcal{P}^{-1}[\mathcal{Q}\mathcal{P}^{-1}\mathcal{Q}\mathcal{P}]\mathcal{P}\mathcal{N}^{-1}
\end{aligned}$$

de lo que podemos sacar,

$$\mathcal{Q}\mathcal{P}^{-1}\mathcal{Q}\mathcal{P} = \mathcal{P}\mathcal{N}^{-1}\mathcal{U}\mathcal{V}\mathcal{N}\mathcal{P}^{-1}$$

Por el mismo razonamiento pero para $\mathcal{VW}$ llegamos a

$$\mathcal{VW} = \mathcal{N}\mathcal{P}^{-2}[\mathcal{Q}\mathcal{P}^{-1}\mathcal{Q}\mathcal{P}]\mathcal{P}^{2}\mathcal{N}^{-1}$$

y ahora sustituimos $\mathcal{Q}\mathcal{P}^{-1}\mathcal{Q}\mathcal{P}$ por $\mathcal{P}\mathcal{N}^{-1}\mathcal{U}\mathcal{V}\mathcal{N}\mathcal{P}^{-1}$,

$$\begin{aligned}
\mathcal{VW} &= \mathcal{N}\mathcal{P}^{-2}\mathcal{P}\mathcal{N}^{-1}\mathcal{U}\mathcal{V}\mathcal{N}\mathcal{P}^{-1}\mathcal{P}^{2}\mathcal{N}^{-1} \\
\mathcal{VW} &= \mathcal{N}\mathcal{P}^{-1}\mathcal{N}^{-1}\mathcal{U}\mathcal{V}\mathcal{N}\mathcal{P}\mathcal{N}^{-1}
\end{aligned}$$

Usando la expresión para $\mathcal{J}$ finalmente tenemos

$$\mathcal{VW} = \mathcal{J}^{-1}\mathcal{U}\mathcal{V}\mathcal{J}$$

Por un método análogo podemos obtener que,

$$\begin{aligned}
\mathcal{WX} &= \mathcal{J}^{-1}\mathcal{VW}\mathcal{J} \\
\mathcal{XY} &= \mathcal{J}^{-1}\mathcal{WX}\mathcal{J} \\
\mathcal{YZ} &= \mathcal{J}^{-1}\mathcal{XY}\mathcal{J}
\end{aligned}$$

Como adelantábamos este conjunto de ecuaciones se usa para determinar $\mathcal{J}$ y luego esta se usa para determinar las 26 posibles $\mathcal{N}$. Utilizando lo visto en el apartado de conjugación.

Además estas 26 posibilidades, en palabras de Rejewski: "No son fundamentalmente diferentes de esta.", refiriéndose a la primera que él descubrió.

Esto se explica ya que el rotor puede estar en 26 posiciones originalmente y eso es lo que crea las 26 posibilidades, pero con más textos interceptados puede deducirse el cableado de este primer rotor sin haberlo visto. Con el tiempo los operarios cambiarían de rotor en posición derecha y al notar esto se empezaría todo el cálculo de nuevo para conocer otro rotor. Tras varios cambios se conocerían los tres rotores de la máquina.

5.2. Ejemplo: hallar el primer rotor

Para comenzar el ejemplo necesitamos haber capturado una gran cantidad de mensajes cifrados con diferentes claves de sesión, de estos Rejewski tenía en abundancia aunque decía que con entorno a ochenta era suficiente. La tabla 1 muestra ochenta claves de sesión distintas y como quedarían estas tras cifrarse con una máquina Enigma M3, de tres rotores, configurada inicialmente en B-I-II-III TFG, es decir, TFG es la clave del día.

Ahora podemos crear las permutaciones $\mathcal{AD}$, $\mathcal{BE}$ y $\mathcal{CF}$ fijándonos en las relaciones entre estas posiciones.

Ejemplo 7. *Vamos a conseguir $\mathcal{AD}$. Para ello buscamos la a en la primera posición y vemos que letra le corresponde en la cuarta. En la fila de clave vrf vemos que a la a le corresponde la u, si repetimos ahora con la u y seguimos, encontramos la cadena:*

$$a \to u \to g \to z \to j \to y \to o \to s \to m \to e \to d \to a$$

Esto crea el ciclo $(a\,u\,g\,z\,j\,y\,o\,s\,m\,e\,d)$.

Ahora repetimos el mismo procedimiento con una letra que no esté en este ciclo, por ejemplo b:

$$b \to k \to l \to q \to w \to n \to v \to h \to i \to t \to x$$

Esto crea el ciclo $(b\,k\,l\,q\,w\,n\,v\,h\,i\,t\,x)$.

Finalmente las letras que faltan, c, f, p y r, son fijas para la permutación $\mathcal{AD}$.

Luego la permutación que buscamos es:

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

Con un proceso análogo conseguimos las otras dos permutaciones compuestas:

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

Como ya dijimos en su momento gracias al servicio de espionaje francés y los fallos de los operarios de las máquinas era fácil conocer alguna de las claves de sesión y con ello alguna de las transposiciones de $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, $\mathcal{D}$, $\mathcal{E}$ y $\mathcal{F}$.

Ejemplo 8. *Supongamos que las claves de sesión cct y abc se repiten mucho y gracias a lo mencionado en el párrafo anterior somos capaces de deducirlas. Además sabemos, porque hemos interceptado muchos mensajes con ellas, que cifradas son, pnm pmb y vti hfa, respectivamente.*

Estas claves significan que $\mathcal{A}$ tiene las transposiciones $(c\,p)$ y $(a\,v)$, $\mathcal{B}$ tiene $(c\,n)$ y $(b\,t)$, $\mathcal{C}$ tiene $(t\,m)$ y $(c\,i)$, $\mathcal{D}$ tiene $(c\,p)$ y $(a\,h)$, $\mathcal{E}$ tiene $(c\,m)$ y $(b\,f)$ y $\mathcal{F}$ tiene $(t\,b)$ y $(c\,a)$.

Clave	ABC	DEF	Clave	ABC	DEF
qay	zlv	jnr	mok	tdd	xsi
wsx	gys	zon	nij	urb	gwl
edc	ioi	tza	buh	ojl	sxs
rfv	fpy	fbe	vzg	amn	udq
tgb	mej	eht	ctf	pbe	pyw
zhn	qxg	wgx	xrd	sik	mez
ujm	nut	vko	yes	kgx	lrh
ikl	eqh	djj	pwa	cvq	cic
okm	bqt	kjo	ome	bzf	kcv
ijn	eug	dkx	cct	pnm	pmb
uhb	nxj	vgt	paw	clp	cnf
zgv	qey	whe	mas	tlx	xnh
tfc	mpi	eba	sun	xjg	bxx
rdx	fos	fzn	mit	trm	xwb
esy	iyv	tor	psy	cyv	cor
wap	glw	znu	xyz	ssu	mtd
ayq	vsa	htg	pqr	cko	cly
sxw	xhp	buf	abc	vti	hfa
dce	hnf	imv	xxx	shs	mun
fvr	rwo	rpy	aaa	vlq	hnc
gbt	wtm	nfb	iii	erc	dwk
hnz	dcu	aad	jjj	lub	qkl
jmu	lzz	qcp	qwe	zvf	jiv
kli	yac	oqk	asd	vyk	hoz
kmo	yzr	ocm	pyx	css	ctn
jni	lcc	qak	yse	kyf	lov
hbu	dtz	afp	xdr	soo	mzy
gvz	wwu	npd	cft	ppm	pbb
fct	rnm	rmb	vgz	aeu	uhd
dxr	hho	iuy	bhu	oxz	sgp
sye	xsf	btv	nji	uuc	gkk
apw	vfp	hvf	mko	tqr	xjm
yqa	kkq	llc	lki	jqc	yjk
xws	svx	mih	mju	tuz	xkp
ced	pgk	prz	nhz	uxu	ggd
vrf	aie	uew	bgt	oem	shb
btg	obn	syq	vfr	apo	uby
nzh	uml	gds	cde	pof	pzv
muj	tjb	xxl	xsw	syp	mof
lik	jrd	ywi	yaq	kla	lng

Tabla 1: conjunto de ochenta claves de sesión

Teniendo suficientes transposiciones podemos conseguir $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, $\mathcal{D}$, $\mathcal{E}$ y $\mathcal{F}$.

Ejemplo 9. *Vamos a obtener $\mathcal{A}$ y $\mathcal{D}$ a partir de $\mathcal{AD}$. Para ello tenemos que colocar los ciclos de igual longitud en dos filas, poniendo el de la segunda fila en orden inverso.*

Siguiendo el ejemplo anterior sabemos que $\mathcal{A}$ tiene las transposiciones $(c\,p)$ y $(a\,v)$. Por otro lado $\mathcal{D}$ tiene $(c\,p)$ y $(a\,h)$. Vamos a usar que ambas tienen $(c\,p)$ para emparejar los ciclos (c) y (p). Eso nos deja los otros dos 1-ciclos, (f) y (r), como la otra pareja.

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

Para conseguir $\mathcal{A}$ reordenamos el 11-ciclo inferior para que en alguna vertical queden a y v, porque $\mathcal{A}$ tiene la transposición $(a\,v)$.

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

Ahora cogiendo las parejas en vertical, en cualquier orden porque son disjuntas, tenemos $\mathcal{A}$ que recordemos consta de trece transposiciones disjuntas.

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

Realizamos los mismos pasos para $\mathcal{D}$ sabiendo que tiene la transposición $(a\,h)$.

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

Con el resto de información y un método análogo al del ejemplo podemos conseguir $\mathcal{B}$ y $\mathcal{E}$ a partir de $\mathcal{BE}$ y haciéndolo una vez más $\mathcal{C}$ y $\mathcal{F}$ a partir de $\mathcal{CF}$.

$$\begin{aligned}\mathcal{B} &= (a\,l)(b\,t)(c\,n)(d\,o)(e\,g)(f\,p)(h\,x)(i\,r)(j\,u)(k\,q)(m\,z)(s\,y)(v\,w)\\\mathcal{E} &= (a\,n)(b\,f)(c\,m)(d\,z)(e\,r)(g\,h)(i\,w)(j\,k)(l\,q)(o\,s)(p\,v)(t\,y)(u\,x)\\\mathcal{C} &= (a\,q)(b\,j)(c\,i)(d\,k)(e\,f)(g\,n)(h\,l)(m\,t)(o\,r)(p\,w)(s\,x)(u\,z)(v\,y)\\\mathcal{F} &= (a\,c)(b\,t)(d\,z)(e\,v)(f\,w)(g\,q)(h\,s)(i\,k)(j\,l)(m\,o)(n\,x)(p\,u)(r\,y)\end{aligned}$$

Con estas permutaciones y $\mathcal{P} = (a\,b\,c\,d\,e\,f\,g\,h\,i\,j\,k\,l\,m\,n\,o\,p\,q\,r\,s\,t\,u\,v\,w\,x\,y\,z)$ podemos calcular $\mathcal{U}$, $\mathcal{V}$, $\mathcal{W}$ y $\mathcal{X}$. Las otras dos permutaciones, $\mathcal{Y}$ y $\mathcal{Z}$, no nos harán falta.

Ejemplo 10. *Calculemos $\mathcal{U}$ según su fórmula, $\mathcal{P}^{-1}\mathcal{A}\mathcal{P}$.*

Cogemos un elemento, por ejemplo la a, y calculamos su imagen por $\mathcal{P}^{-1}\mathcal{A}\mathcal{P}$:

$$a^{\mathcal{P}^{-1}\mathcal{A}\mathcal{P}} = ((a^{\mathcal{P}^{-1}})^{\mathcal{A}})^{\mathcal{P}} = (z^{\mathcal{A}})^{\mathcal{P}} = q^{\mathcal{P}} = r$$
$$a \xrightarrow{\mathcal{P}^{-1}} z \xrightarrow{\mathcal{A}} q \xrightarrow{\mathcal{P}} r$$

Repetimos para el resto de letras y obtenemos:

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

Nota 5. *Al ser $\mathcal{A}$ y $\mathcal{U}$ semejantes, usando $\mathcal{P}$, es natural que tengan la misma estructura en ciclos.*

Las otras permutaciones, $\mathcal{V}$, $\mathcal{W}$ y $\mathcal{X}$, se calculan de la misma forma y cumplen la misma propiedad citada en la nota.

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

Multiplicándolas entre sí conseguimos $\mathcal{U}\mathcal{V}$, $\mathcal{V}\mathcal{W}$ y $\mathcal{W}\mathcal{X}$.

Ejemplo 11. *Calculamos $\mathcal{U}\mathcal{V}$:*

Cogemos un elemento, por ejemplo la a, y calculamos su imagen por $\mathcal{U}\mathcal{V}$:

$$a^{\mathcal{U}\mathcal{V}} = (a^{\mathcal{U}})^{\mathcal{V}} = r^{\mathcal{V}} = h$$
$$a \xrightarrow{\mathcal{U}} r \xrightarrow{\mathcal{V}} h$$

Repetimos este proceso para la h y eventualmente llegamos a tener la cadena:

$$a \to h \to y \to k \to s \to i \to p \to n \to a$$

Es decir, el ciclo $(a\,h\,y\,k\,s\,i\,p\,n)$ forma parte de $\mathcal{U}\mathcal{V}$.

Empezamos de nuevo con otro elemento que no esté en los ciclos que tenemos, por ejemplo la b y conseguiremos uno nuevo $(b\,l\,j\,q\,v)$.

Seguimos hasta agotar los elementos y tendremos que:

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

$(a)(bnyhluzjcpkgxftmev)(drqsoiw)$	$(abojdsplvcqtnzkhmfu)(ew)(gyix)(r)$
$(acrsqubpmgzlwfvdtokiyjexhn)$	$(aducsrtpnbqveykjfwg)(holxizm)$
$(aeznctqwhpomi)(brudvfxjg)(k)(ly)(s)$	$(afymjhqxklzondwibstrvgcue)(p)$
$(agdxl)(btsufzpqyne)(cvhrwji)(km)(o)$	$(ahsvidyoprxmlbugecwknf)(j)(qz)(t)$
$(aiedzrypswlcxngfbvjkoq)(htu)(m)$	$(ajld)(bwmnhuifcyq)(e)(g)(kptv)(orzsx)$
$(akqcztwnighvlefdbxpujmosyr)$	$(alfegihwotxqdc)(byszukr)(jn)(mpv)$
$(amqehxrcbzvnks)(d)(f)(gjoul)(i)(pw)(ty)$	$(anlhyumrdeijpxsb)(c)(fgktzwq)(ov)$
$(aowrejqglikunmscdfhzxt)(b)(pyv)$	$(apzywsdgmtbcekvqh)(filjr)(n)(oxu)$
$(aqimup)(bdh)(cfjselkwt)(gnoyxvr)(z)$	$(arhcgoz)(bemvsfkxwuqjtdinp)(l)(y)$
$(asgpchdjurio)(bflmwvtenqkyz)(x)$	$(atfmxy)(bgqlnrjvusheo)(cipdkz)(w)$
$(autgrk)(bhfnsiqmy)(cjwxzdlo)(ep)(v)$	$(avwyckbirlpfodmzeqnthgsjx)(u)$
$(awzfpgtiskclqoerm)(bjydnuvx)(h)$	$(axcmbkdofqphitjzguw)(eslrnvy)$
$(ayfrogvzhj)(blsmcnw)(dpiux)(etk)(q)$	$(aziv)(bmdqrpj)(cohkfsnxeuygw)(lt)$

Tabla 2: posibles permutaciones $\mathcal{N}$, obtenidas para el ejemplo.

Como siempre, utilizamos un proceso análogo para las otras dos:

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

Con estas tres permutaciones podemos calcular $\mathcal{J}$, para ello utilizamos el siguiente sistema:

$$\begin{cases} \mathcal{VW} = \mathcal{J}^{-1}\mathcal{UVJ} \\ \mathcal{WX} = \mathcal{J}^{-1}\mathcal{VWJ} \end{cases}$$

En este ejemplo $\mathcal{UV}$, $\mathcal{VW}$ y $\mathcal{WX}$, tienen dos 5-ciclos y dos 8-ciclos cada una. Operando nos saldrán entorno a 6400 posibles $\mathcal{J}$ para cada ecuación. Sin embargo, usando el criterio de que la solución debe ser un 26-ciclo, ya que $\mathcal{P}$ lo es y $\mathcal{J}$ es semejante a $\mathcal{P}$, estas posibilidades se reducen. La permutación que buscamos es además la solución única del sistema. Utilizando un programa Java, desarrollado para el cálculo del ejemplo, llegamos a:

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

Como último paso utilizamos la definición de $\mathcal{J}$ como $\mathcal{NPN}^{-1}$ y según la ordenación que escojamos encontramos 26 posibles $\mathcal{N}$ (Tabla 2).

Nota 6. *Como ya adelantábamos en el planteamiento, con varios días de mensajes interceptados se encontrará la verdadera $\mathcal{N}$. Por completitud en este caso la verdadera corresponde a la permutación $(a\,w\,z\,f\,p\,g\,t\,i\,s\,k\,c\,l\,q\,o\,e\,r\,m)(b\,j\,y\,d\,n\,u\,v\,x)(h)$, que está en la duodécima fila de la primera columna.*

Esto se debe a que dependiendo de la configuración de la máquina nos saldrá una $\mathcal{N}$ distinta, pero todas son semejantes entre sí usando $\mathcal{P}$. La $\mathcal{N}$ que tenemos corresponde a la configuración de la máquina en B-I-II-III TFG, es decir, al rotor III en G, llamémosla $\mathcal{N}_g$. Si la comparamos con la "original", $\mathcal{N}_a$, con el rotor III en A, la que tenemos sería $\mathcal{P}^6\mathcal{N}_a\mathcal{P}^{-6}$, semejante.

6. La Bomba de Turing

Entre 1934 y 1940 gracias al catálogo de permutaciones $\mathcal{AD}$, $\mathcal{BE}$ y $\mathcal{CF}$ que creó Rejewski, con la ayuda de Jerzy Rózycki y Henryk Zygalski, y a los pocos cambios que hubo pudieron descifrarse todos los mensajes de los alemanes con poco esfuerzo. Bastaba con reutilizar la teoría anterior una y otra vez.

Pero en 1940 se pierde esta técnica por que se deja de enviar el indicador repetido en los mensajes. Ya que Rejewski, Rózycki y Zygalski huyeron a Paris durante la invasión de Polonia de 1939 el matemático Alan Turing se encargó de encontrar un nuevo método

6.1. Ataques con texto en claro

Los que realizó Turing fueron ataques con texto en claro, es decir, tenían fragmentos de texto en sus dos versiones cifrados y sin cifrar.

Definición 15. *Sea $a_r \dots a_s$ un fragmento de texto en claro y $x_r \dots x_s$ su versión cifrada, al conjunto de ambas lo llamamos puntal o, en inglés, crib.*

Por comodidad vamos a nombrar a la permutación de la máquina Enigma en la i-ésima letra del mensaje (ver Ecuación 1) como $\mathcal{E}_i$. Ya que la permutación $\mathcal{E}_i$ no contaba con el *Steckerbrett*, el panel de conexiones, ahora lo incluimos como una permutación más, $\mathcal{S}$. La fórmula de la i-ésima letra del mensaje, $\hat{\mathcal{E}}_i$, queda entonces:

$$\hat{\mathcal{E}}_i = \mathcal{S}\mathcal{E}_i\mathcal{S}^{-1} \tag{2}$$

Nota 7. *La permutación $\mathcal{S}$ es simétrica por como es el panel de conexiones. Luego $\mathcal{S}$ es igual a $\mathcal{S}^{-1}$.*

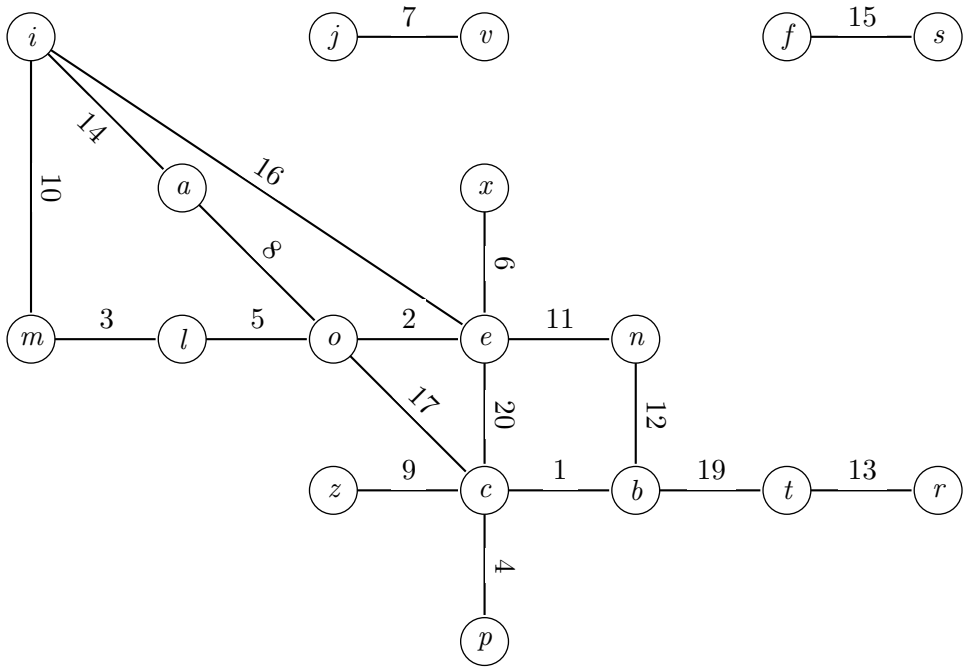
Entonces la relación entre ambas partes de un puntal, marcando lo desconocido en rojo, es la siguiente:

$$a_r \xrightarrow{\mathcal{S}} b_r \xrightarrow{\mathcal{E}_r} b_r^{\mathcal{E}_r} \xrightarrow{\mathcal{S}} x_r$$
$$\dots$$
$$a_s \xrightarrow{\mathcal{S}} b_s \xrightarrow{\mathcal{E}_s} b_s^{\mathcal{E}_s} \xrightarrow{\mathcal{S}} x_s$$

Definición 16. *Si tenemos un puntal, podemos asociarle un grafo cuyos vértices serán las distintas letras que aparecen en el puntal, es decir, $\{a_r \dots a_s\} \cup \{x_r \dots x_s\}$ y sus aristas vienen dadas por las parejas $\{a_i, x_i\}$ con $a_i \neq x_i$ en el puntal. A este grafo lo denominamos menú, es un grafo que tiene como pesos la posición de la primera aparición de la pareja, aunque podría registrarse varias apariciones de la misma pareja con varias aristas entre los mismos vértices y distintos pesos.*

Ejemplo 12. *Supongamos que disponemos del siguiente puntal y obtenemos su menú:*

1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*	*17*	*18*	*19*	*20*
c	*o*	*m*	*p*	*l*	*e*	*j*	*o*	*c*	*i*	*e*	*n*	*t*	*i*	*f*	*i*	*c*	*o*	*t*	*e*
b	*e*	*l*	*c*	*o*	*x*	*v*	*a*	*z*	*m*	*n*	*b*	*r*	*a*	*s*	*e*	*o*	*c*	*b*	*c*



Entre todas las letras pueden darse repeticiones, hecho notable en la incidencia de varias aristas en el mismo vértice. Si se diera el caso de $x_i = a_j$ tendríamos que

$$a_i \xrightarrow{\mathcal{S}} b_i \xrightarrow{\mathcal{E}_i} b_i^{\mathcal{E}_i} \xrightarrow{\mathcal{S}} x_i$$
$$a_j \xrightarrow{\mathcal{S}} b_j \xrightarrow{\mathcal{E}_j} b_j^{\mathcal{E}_j} \xrightarrow{\mathcal{S}} x_j$$

puede expresarse como

$$a_i \xrightarrow{\mathcal{S}} b_i \xrightarrow{\mathcal{E}_i} b_i^{\mathcal{E}_i} \xrightarrow{\mathcal{S}} x_i = a_j$$
$$a_j (= x_i) \xrightarrow{\mathcal{S}} b_j (= b_i^{\mathcal{E}_i}) \xrightarrow{\mathcal{E}_j} b_j^{\mathcal{E}_j} (= b_i^{\mathcal{E}_i \mathcal{E}_j}) \xrightarrow{\mathcal{S}} x_j$$

Con esto podemos ver que si conociéramos configuración de los rotores, $\mathcal{E}_i$ para todo i, pero no el panel de conexiones, $\mathcal{S}$; y una conexión, $\{a_i, b_i\}$, podemos conseguir otra conexión, $\{x_j, b_i^{\mathcal{E}_i \mathcal{E}_j}\}$, ya que $x_j^{\mathcal{S}} = b_i^{\mathcal{E}_i \mathcal{E}_j}$. Repitiendo podemos obtener todas las conexiones respecto a las letras de la componente conexa del menú en la que está a_i.

Al no conocer la configuración de los rotores ni una conexión trabajamos con hipótesis.

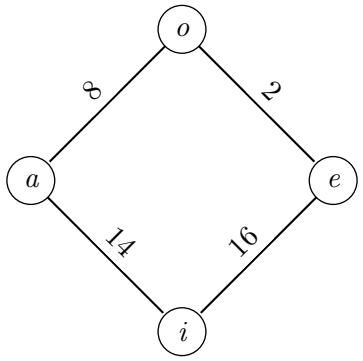
- Asumimos que hay una determinada configuración de rotores lo que nos da unas permutaciones $\mathcal{E}'_1$, $\mathcal{E}'_2$, ... que pueden coincidir, o no, con $\mathcal{E}_1$, $\mathcal{E}_2$, ...
- Asumimos que se da la conexión $\{a_i, b'_i\}$.

Usando el menú podemos calcular las conexiones del resto de letras de la componente conexa de a_i. Si el grafo presenta bucles podemos usarlos para detectar incoherencias con nuestras hipótesis, ya que una letra no puede estar conectada a dos en el tablero de conexiones. Durante el proceso pueden aparecer conexiones incoherentes o podemos llegar a que una de nuestras hipótesis era falsa.

Ejemplo 13. *Volviendo a tomar el mismo puntal, esta vez hacemos dos suposiciones:*

- *La máquina usa una configuración B-I-II-III, anillo en AAA y rotores en ZZZ.*
- *La o está conectada con la z, $o^{\mathcal{S}} = z$.*

Nos vamos a fijar en un bucle que se da en una de las componentes conexas:



Y seguimos la ruta:

$$o \xrightarrow{ZZB} e \xrightarrow{ZZP} i \xrightarrow{ZZN} a \xrightarrow{ZZH} o$$

Nota 8. *Las letras que aparecen sobre las flechas muestran la configuración de los rotores durante la pulsación que les corresponde. Es calculada con la posición en el puntal, el peso de la arista. Por ejemplo la arista entre o y e marca 2, esto significa que haremos 2 pulsaciones, con la primera se pasa del estado inicial ZZZ a ZZA y con la segunda pasamos a ZZB.*

Usando la segunda hipótesis añadimos lo siguiente:

$$\begin{array}{ccccccccccc} & o & \xrightarrow{ZZB} & e & \xrightarrow{ZZP} & i & \xrightarrow{ZZN} & a & \xrightarrow{ZZH} & o & \\ \mathcal{S} & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & \mathcal{S} \\ & z & \xrightarrow{ZZB} & b & \xrightarrow{ZZP} & n & \xrightarrow{ZZN} & p & \xrightarrow{ZZH} & b & \end{array}$$

Nota 9. *Para la segunda línea utilizamos una Enigma sin el panel de conexiones porque queremos usar $\mathcal{E}_i$ que no lo tenía.*

Como resultado vemos que o está conectada con b, pero o ya estaba conectada con z. Nuestra hipótesis es incoherente y no conseguimos ninguna información nueva.

Ejemplo 14. *Repetimos con el mismo puntal, pero ahora con las hipótesis correctas:*

- *La máquina usa una configuración B-I-II-III, anillo en AAA y rotores en ABC.*
- *La o no está conectada con ninguna, $o^{\mathcal{S}} = o$.*

La ruta cambia un poco:

$$o \xrightarrow{ABE} z \xrightarrow{ABS} n \xrightarrow{ABQ} i \xrightarrow{ABK} o$$

Y utilizando la conexión que conocemos:

$$\begin{array}{ccccccccccc} & o & \xrightarrow{ABE} & e & \xrightarrow{ABS} & i & \xrightarrow{ABQ} & a & \xrightarrow{ABK} & o & \\ \mathcal{S} & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & \mathcal{S} \\ & o & \xrightarrow{ABE} & e & \xrightarrow{ABS} & k & \xrightarrow{ABQ} & b & \xrightarrow{ABK} & o & \end{array}$$

Esta vez al no ser incoherente conseguimos como información adicional que la i está conectada con la k, la a con la b y además la e no está conectada con ninguna.

Esto nos lleva a un método de trabajo por fuerza bruta: probamos todas las configuraciones posibles de los rotores y utilizando puntales descartamos las incompatibles o incoherentes, obteniendo de paso algunas conexiones del tablero con las compatibles.

En el ejemplo erróneo vimos que se daba una incoherencia, si repetimos los mismos cálculos para cualquier conexión de o con otras letras encontraremos que si hacemos $o^{\mathcal{S}} = h$ no encontramos incoherencias, este caso se tomaría como compatible y se apuntan las conexiones descubiertas.

Si con otra configuración al crear hipótesis sobre las conexiones no conseguimos ninguna compatible diremos que esa configuración no tiene punto fijo y que es incompatible, la desechamos.

Nota 10. *Antes de seguir vamos a considerar las posiciones de los anillos de los rotores, estos pueden estar en 26^3 posiciones y por cada una de ellas hay 26^3 configuraciones posibles de los rotores, lo que nos da un total de 308915776 posibilidades. Tendríamos que comprobar caso a caso si es compatible con el puntal y, si lo es, deducir conexiones. Podemos mejorarlo con la siguiente observación.*

El anillo sirve para establecer el punto de arrastre entre rotores. Sin embargo, el arrastre no es frecuente y menos dentro de un puntal que abarca una porción pequeña del texto. Así, si el puntal es pequeño o la parte que usamos lo es podemos asumir que no hubo arrastre, podemos olvidarnos del anillo y comprobar solo las $26^3 = 17576$ *configuraciones iniciales de los rotores. Con estas conseguir casos compatibles, pocos si nuestro puntal es lo suficientemente bueno, y deducir parte de la clave.*

6.2. La máquina de Turing

Turing quiso automatizar el proceso y para ello creo una máquina eléctrica, la Bomba. Esta consistía en 36 "máquinas Enigma" (solo se usaban tres rotores sin arrastre y el reflector) agrupadas en tres filas, a doce por fila. En cada "máquina" el rotor superior representa el rotor izquierdo y el inferior al rotor derecho (ver Figura 1). Su función era recorrer los posibles estados de los rotores y comprobar si eran compatibles con un puntal dado.

En uno de los ejemplos del apartado anterior hemos comprobado la compatibilidad del estado inicial ZZZ con el puntal que teníamos utilizando la composición $\mathcal{E}_{ZZB}\mathcal{E}_{ZZP}\mathcal{E}_{ZZN}\mathcal{E}_{ZZH}$, donde $\mathcal{E}_{\alpha\beta\gamma}$ es la permutación de la máquina Enigma, sin arrastre, cuando la ventana de configuración muestra $\alpha\beta\gamma$.

Definición 17. *En teoría de grafos se denomina camino a una secuencia de vértices conectados en un grafo y las aristas que los unen.*

Definición 18. *En teoría de grafos se denomina camino euleriano a un camino que pasa una y solo una vez por las aristas que lo forman.*

Por lo general, escogeremos un camino euleriano del menú para configurar la Bomba, priorizando aquellos más largos y con vértices repetidos. No es importante que el camino empiece y acabe en el mismo vértice. Es necesario, y una característica de la Bomba, que las máquinas Enigma que vamos a usar ahora no efectúan arrastre ni tienen tablero de conexiones.

Al conectar la salida de una Enigma con la entrada de la siguiente conseguimos la composición indicada por nuestro camino euleriano. Configuramos las máquinas como:

- $\alpha\beta\gamma$ la posición base que estamos probando actualmente.
- $\alpha\beta(\gamma + i)$ $_{\text{(mód 26)}}$ con i el peso de la arista del camino.

Nota 11. *α, β y γ son letras para la configuración de Enigma pero podemos operar como si fueran números en módulo 26:*

- $A = 0$, $B = 1$, ...
- $26 \pmod{26} = 0 = A$, $53 \pmod{26} = 1 = B$, ...

En la Bomba iremos cambiando $\alpha\beta\gamma$ hasta agotar las 26^3 posibilidades que hay para la configuración base.

Ejemplo 15. *Supongamos que contamos con 12 Enigmas reducidas, sin arrastre ni tablero de conexiones, vamos a utilizar un camino de 12 aristas del menú anterior.*

$$x \xrightarrow{6} e \xrightarrow{11} n \xrightarrow{12} b \xrightarrow{1} c \xrightarrow{17} o \xrightarrow{5} l \xrightarrow{3} m \xrightarrow{10} i \xrightarrow{14} a \xrightarrow{8} o \xrightarrow{2} e \xrightarrow{16} i$$

Es decir si miramos los estados de la configuración de los rotores, tomando como base $\alpha\beta\gamma$, tendremos:

$$x \xrightarrow{\alpha\beta(\gamma+F)} e \xrightarrow{\alpha\beta(\gamma+K)} n \xrightarrow{\alpha\beta(\gamma+L)} b \xrightarrow{\alpha\beta(\gamma+A)} c \xrightarrow{\alpha\beta(\gamma+Q)} o \xrightarrow{\alpha\beta(\gamma+E)} l$$
$$l \xrightarrow{\alpha\beta(\gamma+C)} m \xrightarrow{\alpha\beta(\gamma+J)} i \xrightarrow{\alpha\beta(\gamma+N)} a \xrightarrow{\alpha\beta(\gamma+H)} o \xrightarrow{\alpha\beta(\gamma+B)} e \xrightarrow{\alpha\beta(\gamma+P)} i$$

e iremos cambiando $\alpha\beta\gamma$.

Para acabar esta sección vamos a introducir los datos de nuestro menú de ejemplo en un simulador de la Bomba, concretamente el de www.lysator.liu.se y veamos si podemos obtener una parada válida, es decir, una sin incoherencias.

Ejemplo 16. *Tenemos nuestro camino euleriano anterior y vamos a tomar dos hipótesis:*

- *La máquina usa una configuración B-I-II-III, anillo en AAA y rotores en ZZZ (= $\alpha\beta\gamma$),*
- *La e está conectada con la a, $e^{\mathcal{S}} = a$.*

Nuestro camino queda de la siguiente forma aplicando la primera hipótesis:

$$x \xrightarrow{ZZF} e \xrightarrow{ZZK} n \xrightarrow{ZZL} b \xrightarrow{ZZA} c \xrightarrow{ZZQ} o \xrightarrow{ZZE} l$$
$$l \xrightarrow{ZZC} m \xrightarrow{ZZJ} i \xrightarrow{ZZN} a \xrightarrow{ZZH} o \xrightarrow{ZZB} e \xrightarrow{ZZP} i$$

Primero trabajamos con la vista frontal (Figura 1), Front, de la Bomba. En ella encontramos las 3 cadenas, chains, de 12 "Enigmas" cada una. Solo vamos a utilizar la primera así que seleccionamos el primer grupo de tres rotores y lo configuramos como I-II-III de arriba a abajo y ZZZ en la posición de los rotores. Luego con el botón Copy to chain lo extendemos a los otros 11. Para acabar en esta vista vamos uno a uno cambiando la configuración del rotor inferior a la letra correspondiente a nuestro camino. Por ejemplo, para el primer grupo debe quedar ZZF así que ponemos F en el tercer rotor.

Ahora cambiamos a la vista lateral izquierda (Figura 2), Left Side, y comprobamos que el primer reflector es el B, que es el que queremos probar.

La siguiente vista a editar es la trasera (Figura 3), Back, donde tenemos que reflejar nuestro camino euleriano. En ella podemos distinguir 3 grupos de conexiones, para las 3

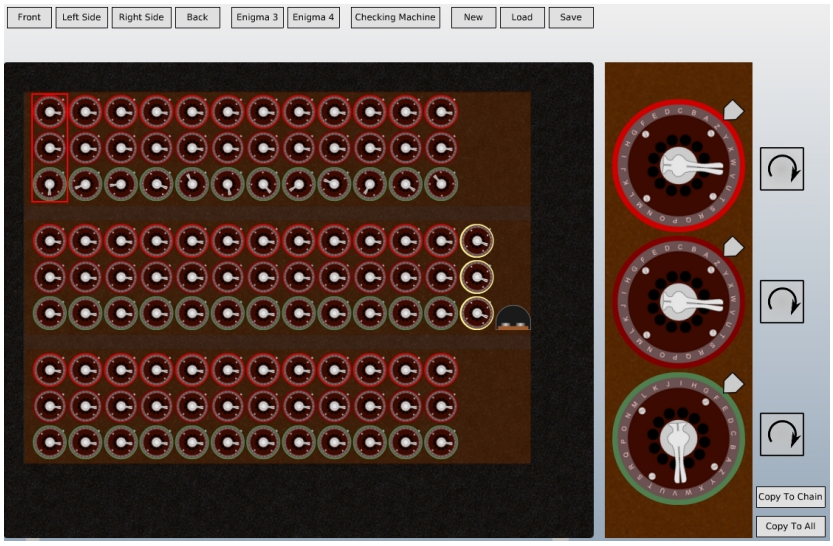


Figura 1: vista frontal de la Bomba, ya configurada

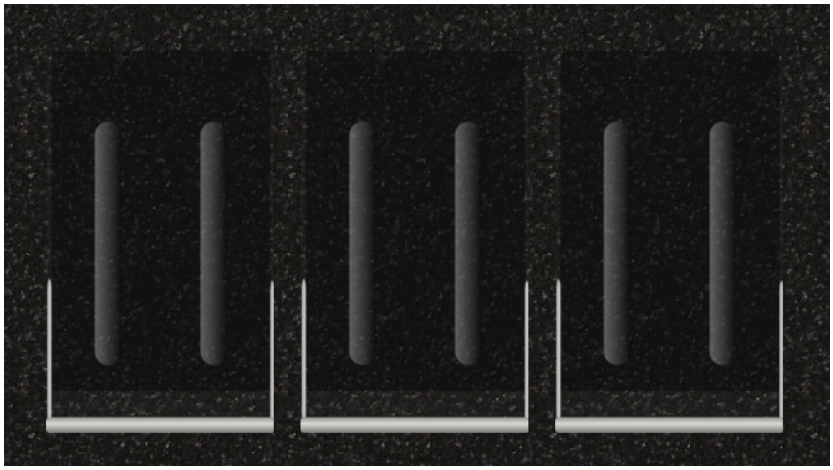


Figura 2: vista lateral izquierda de la Bomba, comprobamos que el primero sea B

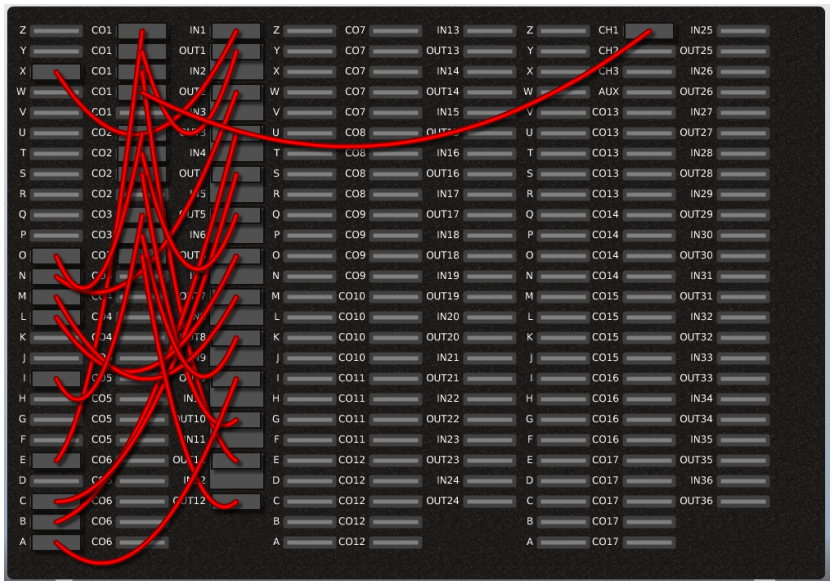


Figura 3: vista trasera de la Bomba, camino reflejado con cables y puentes

cadenas de la Bomba. Como estábamos con la primera cadena trabajaremos con el primer grupo. Para ello al ser un camino primero hacemos puentes entre los conectores OUTi e IN$(i+1)$ *pues la salida de una "Enigma" es la entrada de la siguiente. Tras acabar esto tenemos que conectar con un cable cada letra con su OUT (o IN en el caso de la primera) correspondiente. Por ejemplo, la x se conecta con IN*1 *ya que es la entrada del primer grupo y n se conecta con OUT*2 *pues es la salida del segundo. Si alguna letra tiene repeticiones en el camino primero tenemos que conectarla a un grupo de conectores, los que se llaman CO. Por ejemplo, la e es la salida de los grupos 1 y 11 así que primero la conectamos a un CO*1 *y luego con dos cables desde otros CO*1 *conectamos a OUT*1 *y OUT*11*.*

*Para acabar tenemos que usar la segunda hipótesis, habíamos supuesto que e está conectada con a, para reflejar esto primero donde estamos conectamos un CO*1*, o la letra e, a CH*1 *que marca la entrada para la cadena 1. Como último paso en la vista lateral derecha, Right Side, encontraremos varios interruptores, encendemos los denominados Chain 1, ya que usamos la primera cadena; A en la columna de Chain 1, pues queremos que e, la entrada, esté conectada con a; y Carry para que los rotores avancen por cada revolución completa del anterior. Esta cara de la Bomba es muy grande para hacer una figura, sin embargo, en la Figura 4 encontramos una pantalla interesante en caso de parada.*

Una vez acabada la configuración en la vista frontal tenemos dos botones, el izquierdo enciende la Bomba y el derecho la para. Le damos al botón de la izquierda y comienzan a moverse los rotores.

Cuando se pare tendremos que mirar las vistas frontal y lateral derecha. Nos fijamos en los detalles que destacamos a continuación.

Figura 4: pantalla de la vista lateral derecha, es interesante ver qué letra se ilumina

Figura 5: máquina de verificación, configurada con anillos en YXW, son los puntos negros

- *En la frontal miramos los rotores con borde amarillo para ver la configuración en la que se ha detenido. En la primera parada en nuestro ejemplo se detienen en YXW.*
- *En la lateral derecha encontramos una pantalla (Figura 4) con todas las letras, una de ellas tendrá una barra de luz, la anotamos. En nuestra parada es la E.*

Una vez anotado esto podemos poner a funcionar la Bomba, dándole al botón izquierdo de la vista frontal y levantando la palanca que está a la izquierda de la pantalla en la vista lateral derecha. Entramos por primera vez en la pestaña de la máquina de verificación (Figura 5), Checking machine. Primero la configuramos como el resto de máquinas, reflector B, rotores I-II-III, de izquierda a derecha, y movemos los anillos de los rotores a las letras de la parada, YXW. No hacemos nada con el rotor amarillo, solo sirve para colocar otro más en el caso de trabajar con una Enigma de 4 rotores. Una vez configurada anotamos todas las letras de nuestro camino y a la de entrada, la e, le asignamos la que nos indicaba la pantalla, también la e.

x		*o*
e	*e*	*l*
n		*m*
b		*i*
c		*a*

Ahora, para pasar de la e a la x en nuestro camino tenemos que usar la configuración ZZF, introducimos esta en la máquina de verificación y pulsamos la e, nos saldrá la letra con la que está conectada la x. En nuestro caso es la propia x. Siguiendo todo el camino rellenamos la tabla anterior y queda:

x	x	o	o
e	e	l	l
n	n	m	m
b	a	i	k
c	c	a	b

Es importante notar dos cosas. Primero no hay ninguna contradicción, de hecho es satisfactorio ver que la pareja de la a es la b y viceversa, esto indica que estamos ante un caso válido. Aunque quizás no el correcto. Lo segundo son las conexiones que deducimos de aquí, la a y la b están conectadas, pero también la i y la k.

Nota 12. *Solo vamos a estudiar esta parada, ya que hemos conseguido una válida, pero si se produce otra que produzca incoherencias en este paso, se descarta y esperamos a la próxima parada de la Bomba.*

Vamos a intentar deducir el resto de conexiones a partir de las que tenemos. Primero un resumen de las que sabemos, comparadas con las que hay:

- *Conocemos* (a, b) *e* (i, k)*, el resto se asumen no conectadas entre sí.*
- *Al encriptar el mensaje utilizamos una Enigma configurada como B-I-II-III anillos en AAA y rotores en ABC, además con las conexiones:* (a, b)*,* (d, z)*,* (f, y) *e* (i, k)*.*

Para deducir las que nos faltan vamos a la pestaña Enigma 3 que nos deja configurar una Enigma con lo que sabemos. Colocamos los rotores I-II-III de izquierda a derecha y colocamos sus anillos en YXW. Solo hay que tener en cuenta un detalle, los rotores I, II y III de la Bomba están desfasados con respecto a los de Enigma, van una letra por delante, y por ello en vez de configurarla como ZZZ lo hacemos en YYY. Finalmente las conexiones, en el tablero incluimos las conocidas. Al acabar de configurar tecleamos como si fuéramos un operario que recibe el texto cifrado e intenta desencriptarlo. Lo que sigue es el resultado.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
b	e	l	c	o	x	v	a	z	m	n	b	r	a	s	e	o	c	b	c
c	o	m	p	l	e	j	o	t	i	e	n	t	i	y	i	c	o	t	f

Hemos marcado las letras conflictivas para que sea más visible. Como poseemos la traducción completa de este puntal sabemos que la z de la posición 9 debe corresponder a la

c, y el problema no está en la salida, pues la c de "complejo" ha salido correctamente, debe estar en la entrada. Esto nos da una posible nueva conexión. En la máquina de verificación colocamos ZZI, el correspondiente a la posición 9, y vemos qué letra nos produce una c, esta letra es la d, luego podemos establecer una conexión entre la z y la d, al introducir la z la interpretará como d y por ZZI será una c. Conseguimos:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
b	e	l	c	o	x	v	a	z	m	n	b	r	a	s	e	o	c	b	c
c	o	m	p	l	e	j	o	c	i	e	n	t	i	y	i	c	o	t	f

Repetimos estas correcciones en entradas o salidas para los otros errores. En el caso de la posición 15 teníamos que haber obtenido una f y no una y, probamos si es error en la entrada, pero en ZZO, la permutación de la posición 15, la letra que corresponde la f es la z que ya está unida a la d. Probamos entonces como error de salida y unimos la f y la y. Conseguimos:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
b	e	l	c	o	x	v	a	z	m	n	b	r	a	s	e	o	c	b	c
c	o	m	p	l	e	j	o	c	i	e	n	t	i	f	i	c	o	t	y

Pero el último error no puede solucionarse sin crear nuevos errores o cambiar conexiones que ya tenemos. Además observando las obtenidas son justamente las que se usaron para crear el ejemplo así que el hecho de que todavía encontremos un error en el proceso es que la configuración de los rotores que habíamos supuesto inicialmente no era la correcta.

Como entre parada y parada puede pasar un tiempo considerable, nos interesa saber rápidamente si las paradas son erróneas o válidas, para eso se creo la mejora del teclado diagonal que trataremos a continuación.

6.3. El tablero diagonal y el número de paradas

Antes de introducir el tablero es importante que definamos los hilos y los cables de la Bomba. Así como calcular cuantas paradas hace la Bomba sin él.

Definición 19. *En la Bomba añadimos las letras de nuestro menú. A cada letra la Bomba le hace corresponder un cable. Los cables los denotaremos con letras mayúsculas en azul: A, B, C, ...*

Definición 20. *Cada cable del menú presenta tantos hilos como letras haya en el conjunto inicial, no solo en el menú. Los hilos los denotaremos con subíndices de un cable. Un hilo se dice que está activo si pasa corriente por él.*

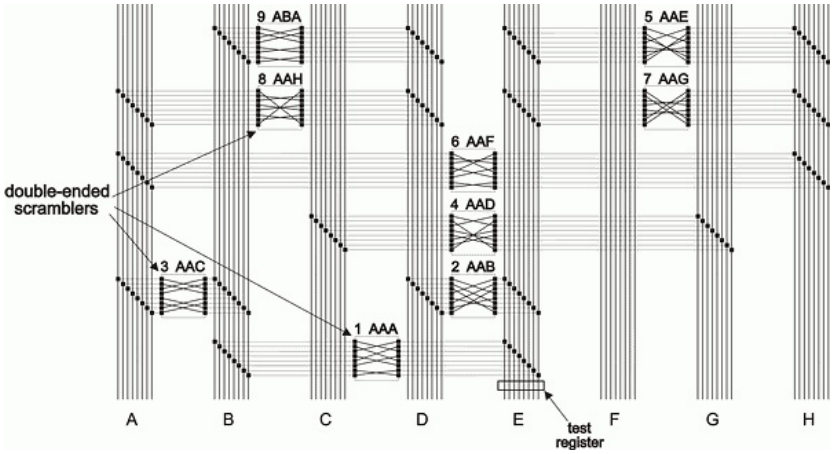


Figura 6: ejemplo de 8 cables con 8 hilos conectados por "Enigmas"

Ejemplo 17. *Si tenemos como conjunto el abecedario de 8 letras y un menú con las letras de la a a la h, tendremos 8 cables y cada cable tendrá 8 hilos (Figura 6).*

$$\begin{aligned} &\textit{Los hilos del cable } A: \ A_a,\ A_b,\ \ldots,\ A_h \\ &\textit{Los hilos del cable } B: \ B_a,\ B_b,\ \ldots,\ B_h \\ &\ldots \\ &\textit{Los hilos del cable } H: \ H_a,\ H_b,\ \ldots,\ H_h \end{aligned}$$

Los hilos de los cables estarán conectados entre sí por las "Enigmas" de la Bomba según como la configuremos y el menú con el que estemos trabajando para ello.

Es importante saber que si un cable cualquiera $\mathcal{X}$, tiene un hilo cualquiera, $\mathcal{X}_\alpha$, activo. Significa que hay una conexión en el tablero entre las letras que representan $\mathcal{X}$ y α.

La ventana de control es un panel en el que se puede ver cuantos hilos activos tiene un cable, en el ejemplo de la sección anterior la ventana estaba en el lateral derecho de la máquina y estaba puesta sobre el cable de entrada a la cadena 1, es decir, al cable E.

Nota 13. *Debido a que asumimos que nuestro menú es conexo, si un cable tiene n hilos activos, entonces todos los cables tienen n hilos activos. Las "Enigmas" propagan la señal hasta que se cumple esto.*

Normalmente para contar los hilos activos tras la propagación la ventana de control se pone en el cable por el que se introdujo la señal a la cadena. Pero esto da igual ya que todos tendrán el mismo número. Solo es necesario que sepamos a qué cable estamos poniéndole la ventana por si llegamos a una parada válida saber qué conexiones deducimos.

Nota 14. *Para detectar ahora una parada válida nos basta saber que hay un solo hilo activo en la ventana de control, tras la propagación.*

Nota 15. *Si en lugar de solo un hilo activo nos quedan todos menos uno, estamos ante un caso contradictorio. Sin embargo, su opuesto, es decir, introducir la señal por el hilo no activo, nos daría un caso válido, pues los circuitos no se conectan.*

Estas observaciones nos hacen ver que tras inyectar la señal podemos encontrar varias situaciones:

1. Solo hay un hilo activo en la ventana de control. Debemos efectuar una parada y considerarla.
2. Solo hay un hilo no activo en la ventana de control. Si estamos probando todos los hilos podemos no parar, al llegar al hilo no activo se dará el caso 1. Pero, si no estamos probando todos los hilos debemos parar y considerar su opuesto.
3. Hay un número distinto a 1 o 25 de hilos activos en la ventana de control. En cualquier caso se salta por ser contradictoria, pero si no se están probando todos los hilos podemos saltarnos la clave correcta.

Teniendo en cuenta esto, sabemos cuando va a parar, o debería parar, la Bomba, así que ya podemos calcular el número de paradas, sin teclado diagonal, en dos casos: con y sin ciclos. Siempre probaremos todos los hilos para no correr el riesgo de perder la clave correcta.

Paradas de la Bomba sin ciclos

Al no tener ciclos nunca hay retorno de la señal al cable de entrada, entonces solo hay 1 hilo activo en cada cable, siempre se para. Al tener 3 rotores con 26 estados cada uno y 26 hilos esto genera 26^4 paradas.

Paradas de la Bomba con ciclos

Al añadir un ciclo, entre dos cables, al menú hacemos que solo en 1 de cada 26 veces el hilo activo de un cable se conecte con el hilo activo del otro. Si se conectara un hilo activo del primero y uno no activo del segundo o viceversa se produciría una propagación de la señal que aumentaría el número de hilos activos y por lo tanto no se pararía.

Entonces en el caso de que no se añadan nuevos hilos activos hemos reducido el número de paradas mediante el factor $\frac{1}{26}$ por añadir un ciclo. Añadir nuevos ciclos sigue reduciendo por el mismo factor y al final el número de paradas es

$$26^{4-C}$$

donde C es el número de ciclos "independientes" del menú.

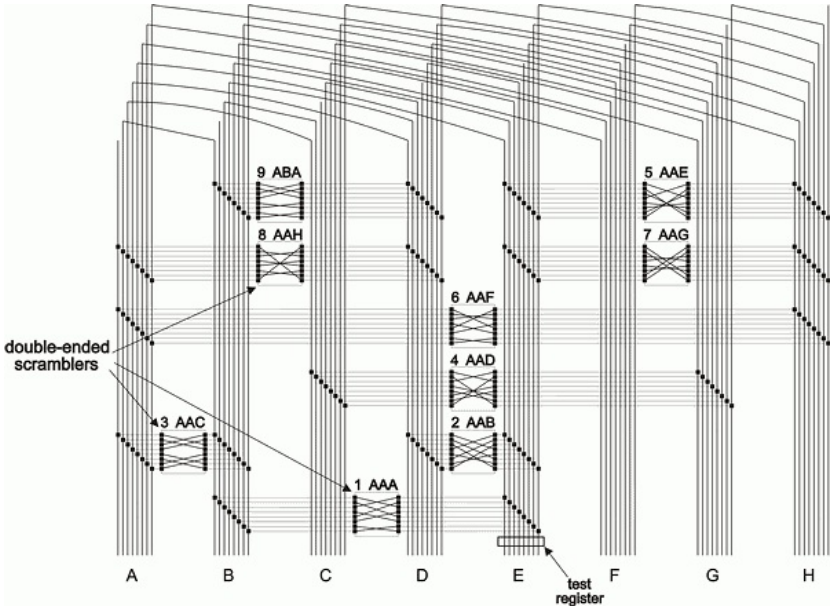


Figura 7: ejemplo de 8 cables con 8 hilos conectados por "Enigmas" y tablero diagonal

Definición 21. *En la teoría de grafos se llama ciclos fundamentales o independientes a aquellos que poseen al menos una arista distinta al resto de ciclos fundamentales.*

Proposición 2. *En un grafo con m aristas, n vértices y c componentes conexas hay exactamente*

$$m - n + c$$

ciclos independientes.

Definición 22. *Al número de ciclos independientes de un grafo se le llama corrango.*

Visto este número de paradas que tomamos como base y que es elevado si tenemos pocos ciclos, vamos a presentar el tablero diagonal (Figura 7).

El tablero lo único que hace es asegurar una consecuencia lógica, si x está conectado con y, en el tablero de conexiones, entonces el recíproco también debe ser cierto.

Ejemplo 18. *Veamos como conecta el cable $\mathcal{X}$ con el resto de cables. Para ello conecta todos los hilos del cable $\mathcal{X}$ con los correspondientes en otros cables siguiendo las reglas:*

- *El hilo $\mathcal{X}_y$ lo conecta con el hilo $\mathcal{Y}_x$, del cable $\mathcal{Y}$, para todo y del conjunto.*
- *El hilo $\mathcal{X}_x$ lo deja sin conectar, ya estamos en el cable $\mathcal{X}$.*

Nos permite detectar incoherencias más rápido que si no lo tuviésemos.

Ejemplo 19. *Veamos como detectamos una incoherencia desde la ventana de control gracias al teclado diagonal.*

Sean los cables $\mathcal{X}$ y $\mathcal{Y}$ conectados en el menú y por lo tanto tienen una "Enigma", que denominaremos $\mathcal{E}$, entre ellos. Supongamos que $y^{\mathcal{E}} = \alpha$

Introducimos una señal eléctrica por el hilo $\mathcal{X}_y$, esta señal llega a dos hilos del cable $\mathcal{Y}$: al hilo $\mathcal{Y}_\alpha$ por la máquina "Enigma" y al hilo $\mathcal{Y}_x$ por el tablero diagonal. Pueden darse dos situaciones:

- *Los hilos coinciden, es decir, $\alpha = x$ y no hay incoherencia.*
- *Los hilos no coinciden, tendremos 2 hilos activos en $\mathcal{Y}$ y esto se extenderá al resto de cables, luego no se producirá una parada.*

Esto era solo un ejemplo para ilustrar que hay falsas paradas que pueden ser detectadas y evitadas con el tablero diagonal. Ahora procedemos a considerar los casos en los que ayuda y calcular en cuanto mejora el número de paradas.

Paradas de la Bomba con teclado diagonal

Ya que paramos cuando hay solo un hilo activo por cable y el tablero diagonal añade conexiones es de esperar que el número de paradas se reduzca al ser probable que aumente el número de hilos activos. Es decir, una parada sin el tablero será válida si al añadirlo no aparecen hilos activos nuevos.

Para estudiar los distintos casos utilizaremos que en nuestro alfabeto hay 26 letras y suponemos que tenemos un menú de N letras. También admitimos que antes de añadir el tablero diagonal estabamos en una parada, es decir, teníamos solo un hilo activo por cada cable del menú. Al colocar el tablero no se crean nuevos hilos activos en tres circunstancias. En estas el hilo activo de un cable cualquiera del menú, $\mathcal{X}$:

1. Está conectado por el tablero diagonal al hilo activo de otro cable del menú.
2. Corresponde a sí mismo, es decir, el hilo activo es $\mathcal{X}_x$.
3. Está conectado a una letra fuera del menú.

Diremos que un cable es de tipo 1 si se da el caso 1 y de forma análoga para el resto de casos.

La probabilidad de los casos 2 y 3 es fácilmente calculable como veremos a continuación.

- En el caso 2 solo 1 de 26 hilos puede estar activo, luego, la probabilidad de que suceda es $\frac{1}{26}$.
- En el caso 3 nuestro cable $\mathcal{X}$ puede estar conectado a $26 - N$ cables que no están en el menú, luego, la probabilidad de que suceda es $\frac{26-N}{26}$.

Nos centraremos pues en la probabilidad del caso 1. Como los casos 1, 2 y 3, son excluyentes el otro cable al que está conectado $\mathcal{X}$ también se encuentra en el caso 1. Los cables de tipo 1 van por parejas.

Sabiendo esto podemos pensar cual es la probabilidad de que M de los N cables del menú sean de tipo 1, y es:

$$\frac{M-1}{26^2}\frac{M-3}{26^2}\cdots\frac{1}{26^2}$$

Esto tiene dos observaciones:

- M es par, como hemos dicho estos cables van por parejas.
- La probabilidad de que un cable de tipo 1 conecte su hilo activo con otro de los $M-1$ cables restantes de tipo 1 es $\frac{M-1}{26}$ y de que coincida justo en el hilo activo de ese cable es $\frac{M-1}{26^2}$. Para el resto quitamos la pareja de cables ya establecida y por eso empezamos con $M-2$ cables de tipo 1, tras la segunda pareja con $M-4$, ...

Juntando los tres casos en una misma fórmula podemos ver cual es la probabilidad de que incluir el tablero diagonal no añada nuevos hilos activos a los cables de nuestro menú. A esta probabilidad la vamos a llamar V y es la probabilidad de que una falsa parada no sea detectada por el tablero diagonal. Turing llamó a este factor $H - M$ y lo estimó. En la Tabla 3 los comparamos.

La fórmula para el cálculo de V, suponiendo que dentro de los N cables del menú tenemos $2i$ de tipo 1, j de tipo 2 y k de tipo 3, es:

$$\begin{aligned}
V &= \sum_{\substack{2i+j+k=N\\ i,j,k\geq 0}} \frac{(2i-1)(2i-3)\ldots 1}{26^{2i}}\frac{1}{26^j}\frac{(26-N)^k}{26^k}\binom{N}{2i,j,k} \\
&= \frac{1}{26^N}\sum_{\substack{2i+j+k=N\\ i,j,k\geq 0}} (26-N)^k\frac{(2i)!}{2^i i!}\frac{N!}{2i!k!(N-2i-k)!} \\
&= \frac{N!}{26^N}\sum_{2i+k\leq N}\frac{(26-N)^k}{2^i i!k!(N-2i-k)!}
\end{aligned}$$

Utilizando distintos valores de N conseguimos la Tabla 3.

N	V	$H-M$
2	0.926	0.92
3	0.791	0.79
4	0.619	0.62
5	0.443	0.44
6	0.287	0.29
7	0.168	0.17
8	0.0878	0.87
9	0.0407	0.041
10	0.0166	0.016
11	0.00590	0.0060
12	0.00180	0.0018
13	0.000466	0.00045
14	0.000101	0.000095
15	0.0000179	0.000016
16	0.00000257	0.0000023

Tabla 3: valor de V y el factor $H-M$ de Turing para distintos valores de N.

C \ N	8	9	10	11	12	13	14	15	16
3	2	1	0	0	0	0	0	0	0
2	59	28	11	4	1	0	0	0	0
1	1543	716	292	104	32	8	2	0	0
0	40108	18611	7592	2695	823	213	46	8	1

Tabla 4: número de paradas según valores de C y N, con el factor V

.

Teniendo esta probabilidad calculada, obtener el número de paradas de la Bomba con el tablero diagonal instalado sería multiplicar por V el antiguo, es decir,

$$26^{4-C}V$$

sería el nuevo número de paradas.

Dándole valores a C y a N, pues V depende de N, podemos tabular cuantas paradas hará la Bomba, redondeando al entero más próximo (Tabla 4).

Otro caso de parada

Si revisamos el caso 3 anterior veremos que todavía hay unas paradas falsas que podíamos haber evitado. Estas suceden cuando al menos dos cables del menú tienen conectados sus hilos activos al mismo cable exterior al menú. Evidentemente es una contradicción pero nuestro caso 3 no la detectaba.

C \ N	8	9	10	11	12	13	14	15	16
3	1	0	0	0	0	0	0	0	0
2	13	4	1	0	0	0	0	0	0
1	344	93	20	3	0	0	0	0	0
0	8940	2428	522	89	12	1	0	0	0

Tabla 5: Número de paradas según valores de C y N, con el factor W

.

Para ello se utilizaron aparatos que detectaban estas condiciones y saltaban esta parada. Uno de ellos se llamaba *machine gun*, ametralladora en inglés. Ante una situación de parada comprobaba todos los cables rápidamente haciendo un sonido similar al del arma. Gracias a su estructura detectaba justo esta falsa parada y hacia continuar a la Bomba.

Como nos interesa calcular el nuevo número de paradas tras esta consideración vamos a cambiar el caso 3 anterior por el caso 3'. El caso 3' sucede si un cable del menú tiene su hilo activo conectado a un cable externo al menú que no tenga hilos activos previos.

La probabilidad de que tengamos k de estos cables cambia, ya no es $\left(\frac{26-N}{26}\right)^k$ sino

$$\frac{26-N}{26}\frac{25-N}{26}\cdots\frac{27-k-N}{26}$$

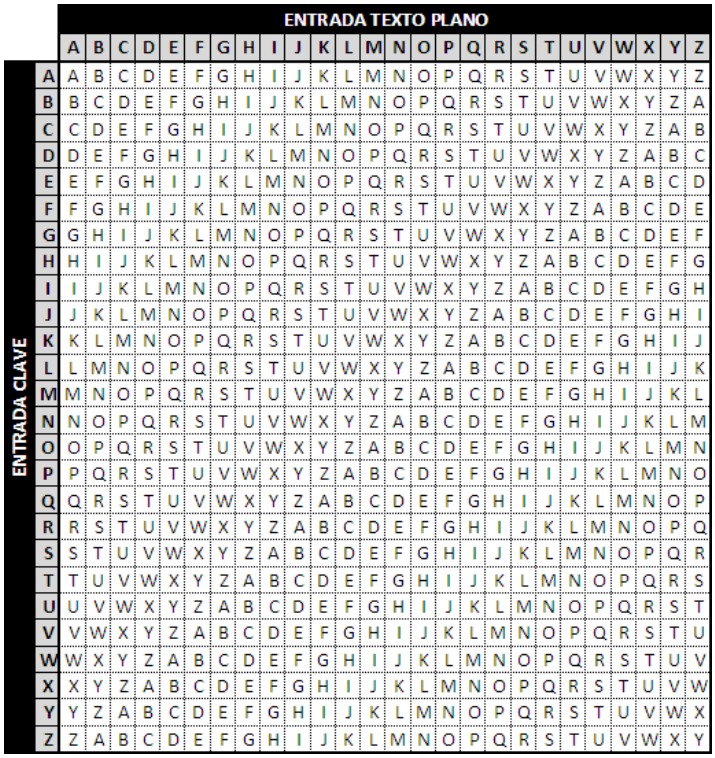
Con este cambio calculamos una nueva probabilidad de manera similar a como calculamos V. Un nuevo factor, al que llamaremos W. Su fórmula es

$$W = \frac{N!}{26^N}\sum_{2i+k\leq N}\frac{(26-N)\ldots(27-k-N)}{2^i i!k!(N-2i-k)!}$$

y el número de paradas es $26^{4-C}W$. Hemos tabulado para este factor el número de paradas esperado (Tabla 5), según los valores de C y N. La nueva, obviamente, mejora la anterior (Tabla 4), al ser W menor que V.

7. Análisis estadístico

En esta última sección vamos a hablar un poco más sobre probabilidades y estadística a la hora de atacar un texto cifrado. Primero empezaremos con un ejemplo sobre como hacer criptoanálisis del cifrado Vigenère y luego introduciremos la teoría y definiciones de Claude Shannon que influenció el estudio científico de la criptografía con su artículo *Communication Theory of Secrecy Systems*.



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

Figura 8: tabla de Vigenère

Criptoanálisis para Vigenère

Vamos a presentar el cifrado propuesto por Blaise de Vigenère, aunque fue creado por Giovan Battista Belasso, para posteriormente atacarlo.

Este algoritmo se basa en otro cifrado famoso, el cifrado César utilizado por los romanos. El último es un simple algoritmo de cifrado por sustitución, se escoge una letra, x_i, y se hace corresponder la a con ella, la b con la siguiente a x_i y así sucesivamente.

Vigenère aumenta la complejidad del cifrado, añadiendo una clave y convirtiéndolo así en uno de sustitución polialfabético. Se basa en el César porque para cifrar con Vigenère se utilizaba una tabla, la tabla de Vigenère (Figura 8), en la que se escribían todos los cifrados César posibles.

Con la clave y el mensaje se hacía lo siguiente: se repetía la clave hasta llegar al mismo número de letras del mensaje, para cada par de letras de la clave repetida y del mensaje se buscaba la fila y la columna de la tabla de Vigenère correspondiente y por último se escribía como mensaje cifrado la letra que aparecía en la tabla.

Ejemplo 20. *Queremos encriptar la palabra* ***matematicas*** *usando la clave* ***grado****. Evitamos la tilde por no tenerla en el alfabeto que consideramos.*

Primero repetimos la clave hasta lograr el mismo número de letras:

$$m\ a\ t\ e\ m\ a\ t\ i\ c\ a\ s$$
$$g\ r\ a\ d\ o\ g\ r\ a\ d\ o\ g$$

Luego buscamos la primera pareja, m y g, en la tabla y conseguimos una s, la primera letra de nuestro mensaje encriptado. Al repetir para el resto de parejas tendremos la palabra ***srthagkifoy****. Para desencriptar usamos el resultado en vez de matematicas.*

Para atacar el cifrado Vigenère, que se llamó "código indescifrable", hay que realizar dos pasos, primero determinamos la longitud de la clave, la denotaremos con M, y posteriormente intentaremos deducirla.

Para la longitud de la clave hay varias técnicas, pero explicaremos el método de Kasiski y el índice de coincidencia.

Para el primero es importante que observemos, en el texto cifrado, varias repeticiones de tres o más letras. Esto puede haberse producido al cifrar de igual forma segmentos iguales del texto en claro. También mediremos las distancias entre estas repeticiones, siendo δ_i la distancia entre el segmento i y el $i+1$. Podemos suponer que M divide todas las distancias y por ello también al máximo común divisor de las mismas.

Ahora veamos el otro método.

Definición 23. *Sea $\boldsymbol{x} = x_1 x_2 \dots x_N$ una cadena de N letras. El índice de coincidencia de la cadena es la probabilidad de que dos elementos de ella sean idénticos. Se denota por $I_c(\boldsymbol{x})$.*

Utilizaremos las frecuencias de las diferentes letras del alfabeto, a las que denominamos f_i, frecuencia de la i-ésima letra, empezando en 0 para la a y acabando en 25 para la z. Hay $\binom{N}{2}$ maneras de escoger 2 elementos de $\mathbf{x}$. Sin embargo, para cada i entre 0 y 25, solo hay $\binom{f_i}{2}$ de que ambos sean i, siendo aquí i un número pero corresponde a la i-ésima letra del abecedario.

Con todo esto el índice de coincidencia para una cadena o texto de longitud N, $\mathbf{x}$, se calcula como:

$$I_c(\mathbf{x}) = \frac{\sum_{i=0}^{25} \binom{f_i}{2}}{\binom{N}{2}} = \frac{\sum_{i=0}^{25} f_i(f_i-1)}{N(N-1)}$$

Letra	Probabilidad	Letra	Probabilidad
a	0.082	n	0.067
b	0.015	o	0.075
c	0.028	p	0.019
d	0.043	q	0.001
e	0.127	r	0.060
f	0.022	s	0.063
g	0.020	t	0.091
h	0.061	u	0.028
i	0.070	v	0.010
j	0.002	w	0.023
k	0.008	x	0.001
l	0.040	y	0.020
m	0.024	z	0.001

Tabla 6: Probabilidad de cada letra en un texto en inglés

.

No obstante, cuando hablamos de un idioma puede estudiarse la probabilidad de cada letra, por palabras que la contengan, uso de esas palabras y observaciones relacionadas. Así se crean tablas como la 6, que tiene estas probabilidades para el inglés, las llamaremos p_i para diferenciarlas de las f_i aunque esencialmente son lo mismo. El índice de coincidencia suele aproximarse por

$$I_c(\mathbf{x}) \approx \sum_{i=0}^{25} p_i^2$$

que con las probabilidades del inglés nos da 0.066.

Definido el índice ahora empezamos con el método que lo acompaña para determinar la longitud de la clave de un texto de longitud N, $\mathbf{x} = x_1 x_2 \dots x_N$, en inglés.

Primero establecemos una longitud de clave a probar, por ejemplo sigamos con M, entonces las letras separadas entre sí M posiciones se han cifrado con el mismo desplazamiento. Las agrupamos en M distintas cadenas a las que llamaremos:

$$y_i = x_i \; x_{M+i} \; x_{2M+i} \dots$$

con i entre 1 y M. No siempre son cadenas de igual longitud, pero no importa.

Ejemplo 21. *Tenemos un texto con 9 letras $x_1 x_2 \dots x_9$. Si creemos que tiene una clave de 3 letras las cadenas quedan:*

$$y_1 = x_1 x_4 x_7 \quad y_2 = x_2 x_5 x_8 \quad y_3 = x_3 x_6 x_9$$

Pero si queremos probar con una clave de 4 letras las cadenas quedan:

$$y_1 = x_1 x_5 x_9 \quad y_2 = x_2 x_6 \quad y_3 = x_3 x_7 \quad y_3 = x_4 x_8$$

Si la clave es de longitud M entonces es de esperar que $I_c(y_i)$ sea cercano a 0.066, para todo i. Si M no es la longitud las cadenas son más aleatorias pues cada una ha usado una encriptación diferente, entonces su índice será más próximo al de un alfabeto, de 26 letras, completamente aleatorio, es decir,

$$I_c(y_i) \approx \sum_{i=0}^{25} \left(\frac{1}{26}\right)^2 = 26\left(\frac{1}{26}\right)^2 = \frac{1}{26} = 0{,}038$$

para todo i.

Los valores 0.066 y 0.038 están lo suficientemente separados para verificar si nuestra hipótesis del método de Kasiski es válida utilizando el método del índice de coincidencia.

Nota 16. *En el caso del español el índice de coincidencia es de 0.072.*

Una vez sabemos la longitud de la clave, o asumimos que hemos encontrado la correcta, nos toca determinar la clave, $k = k_1k_2 \dots k_M$. Para esto hay un método sencillo. Se aplica una vez por cada cadena creada en el método del índice de coincidencia:

1. Calculamos la frecuencia de cada letra en la cadena y_i. Consideramos que f_0 es la frecuencia de la a, f_{25} la de la z.
2. Calculamos $N' = N/M$ que es la longitud de la cadena.
3. Creamos la distribución de probabilidad para la cadena:
$$\frac{f_0}{N'}, \dots, \frac{f_{25}}{N'}$$
4. La cadena y_i fue encriptada con un algoritmo de desplazamiento de k_i, lo que transforma la distribución anterior en:
$$\frac{f_{k_i}}{N'}, \dots, \frac{f_{25+k_i}}{N'}$$
trabajando en módulo 26 en los subíndices.
5. Sea $0 \leq G \leq 25$ trabajamos con la cantidad:
$$M_G = \sum_{i=0}^{25} \frac{p_i f_{i+G}}{N'}$$
6. Si $G = k_i$ entonces se cumple que:
$$M_G \approx \sum_{i=0}^{25} p_i^2 = 0{,}066$$

Esto nos ayuda a obtener cada k_i y con todos reconstruimos la clave. Con esto se acaba de superar el cifrado Vigenère.

Nota 17. *En los pasos anteriores se trata G y k_i como si fueran números, pero recordamos que se mueven entre 0 y 25 y siempre mantienen una relación con el abecedario, siendo a la letra correspondiente al 0 y z la correspondiente al 25.*

7.1. La teoría de Shannon

Una vez visto que la estadística nos ayuda a la hora de enfrentarnos a tipos de cifrados vamos a hablar de la teoría de Claude Shannon, matemático, ingeniero eléctrico y criptógrafo conocido como el padre de la teoría de la información.

Teoría elemental de probabilidad

Damos unas cuantas definiciones y resultados de la teoría de probabilidad para utilizar la notación más adelante.

Definición 24. *Sea $\mathcal{X}$ una variable aleatoria discreta, sobre un conjunto finito X y que tiene una distribución de probabilidad definida en X. La probabilidad de que $\mathcal{X}$ tome el valor x se denota con $P[\mathcal{X} = x]$ o de manera abreviada $P[x]$ si está claro que hablamos de $\mathcal{X}$.*

Debe darse que $P[x] \geq 0$ para todo x en X y

$$\sum_{x \in X} P[x] = 1$$

Definición 25. *Sean $\mathcal{X}$ e $\mathcal{Y}$ variables aleatorias sobre conjuntos finitos, X e Y respectivamente. La probabilidad de que $\mathcal{X}$ tome el valor x e $\mathcal{Y}$ tome el valor y se denomina probabilidad conjunta y se denota $P[x, y]$.*

Definición 26. *Sean $\mathcal{X}$ e $\mathcal{Y}$ variables aleatorias sobre conjuntos finitos, X e Y respectivamente. La probabilidad de que $\mathcal{X}$ tome el valor x dado que $\mathcal{Y}$ toma el valor y se denomina probabilidad condicionada y se denota $P[x|y]$.*

Definición 27. *Sean $\mathcal{X}$ e $\mathcal{Y}$ variables aleatorias sobre conjuntos finitos, X e Y respectivamente, tales que $P[x, y] = P[x]P[y]$ para todo x en X e y en Y. Se dice que $\mathcal{X}$ e $\mathcal{Y}$ son variables independientes.*

Proposición 3. *Sean $\mathcal{X}$ e $\mathcal{Y}$ variables aleatorias sobre conjuntos finitos, X e Y respectivamente. Las probabilidades conjunta y condicionada se relacionan mediante las fórmulas:*

$$P[x, y] = P[x|y]P[y] = P[y|x]P[x]$$

De estas expresiones se obtienen el siguiente teorema y su corolario.

Teorema 8. *(Teorema de Bayes) Sean $\mathcal{X}$ e $\mathcal{Y}$ variables aleatorias sobre conjuntos finitos, X e Y respectivamente. Si $P[y]>0$, entonces*

$$P[x|y] = \frac{P[y|x]P[x]}{P[y]}$$

Corolario 1. *$\mathcal{X}$ e $\mathcal{Y}$ son variables aleatorias independientes si y solo si $P[x|y] = P[x]$ para todo x en X e y en Y.*

Con estas definiciones y resultados podemos enfrentarnos a los conceptos que proponía Shannon. Para ello vamos a necesitar además la noción de criptosistema.

Definición 28. *Un criptosistema es la agrupación de 5 conjuntos: textos planos o claros posibles, a este conjunto lo llamamos $\mathcal{P}$; textos cifrados posibles, lo llamamos $\mathcal{C}$; posibles claves a utilizar, lo llamamos $\mathcal{K}$; funciones posibles para la encriptación, lo llamamos $\mathcal{E}$; y funciones posibles para el proceso inverso, lo llamamos $\mathcal{D}$. Se cumple lo siguiente.*

- *Las funciones $E_k \colon \mathcal{P} \to \mathcal{C}$ con $k \in \mathcal{K}$ pertenecen a $\mathcal{E}$.*
- *Las funciones $D_k \colon \mathcal{C} \to \mathcal{P}$ con $k \in \mathcal{K}$ pertenecen a $\mathcal{D}$.*
- *Para cada $e \in \mathcal{K}$, existe $d \in \mathcal{K}$ tal que $D_d(E_e(p)) = p$ para todo $p \in \mathcal{P}$.*

Así un criptosistema se denota $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$

Secreto perfecto

Si tenemos un criptosistema, $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, tal que se escoge una clave diferente, $k \in \mathcal{K}$, para cada carácter del texto plano, aleatoriamente de entre todas las de $\mathcal{K}$, entonces la clave es una variable aleatoria, la llamaremos K. También podemos recordar que el texto en claro tiene una distribución de probabilidad en $\mathcal{P}$. Llamamos a la variable aleatoria de que $x \in \mathcal{P}$ suceda en el texto en claro X. Además como estamos escogiendo la clave sin importarnos el texto podemos asumir que K y X son variables independientes.

Las distribuciones de probabilidad en $\mathcal{P}$ y $\mathcal{K}$ inducen otra en $\mathcal{C}$, entonces podemos establecer una variable aleatoria para la probabilidad de que el texto cifrado resultante sea $y \in \mathcal{C}$, a esta la llamamos Y. Se verifica la fórmula

$$P[Y = y] = \sum_{\{k \colon y \in C(k)\}} P[K = k]P[X = D_k(y)]$$

donde $C(k) = \{E_k(x) \colon x \in \mathcal{P}\}$ es el conjunto de posibles textos cifrados para una clave $k \in \mathcal{K}$ y E_k es una función de encriptación para la clave k y D_k la de desencriptación para la misma.

Con esta podemos considerar la probabilidad de que y sea el texto cifrado cuando nos dicen que x es el texto plano,

$$P[Y = y|X = x] = \sum_{\{k:\ x=D_k(y)\}} P[K = k]$$

y utilizando ambas, y el teorema de Bayes, la de que x sea el texto plano cuando y es el texto plano,

$$P[X = x|Y = y] = \frac{P[X = x] \sum_{\{k:\ x=D_k(y)\}} P[K = k]}{\sum_{\{k:\ y\in C(k)\}} P[K = k]P[X = D_k(y)]}$$

Definición 29. *Sea $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ un criptosistema en el que $P[x|y] = P[x]$ para todos $x \in \mathcal{P}$ e $y \in \mathcal{C}$. Se dice que el criptosistema tiene secreto perfecto.*

Esto equivale a que la probabilidad de que el texto plano sea x sabiendo que y es el cifrado coincide con la probabilidad de que sea x sin saber nada.

Un texto en el que cada carácter haya sido encriptado con una clave escogida aleatoriamente y secreto perfecto no puede ser descifrado sin conocer las claves que se han utilizado. No puede atacarse.

Shannon profundizó en el concepto de secreto perfecto llegando a una caracterización si se da el caso de que $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$.

Teorema 9. *Sea $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ un criptosistema en el que $|\mathcal{P}| = |\mathcal{C}| = |\mathcal{K}|$. Entonces el criptosistema tiene secreto perfecto si y solo si cada clave es usada con la misma probabilidad, $\frac{1}{|\mathcal{K}|}$ y para cada $x \in \mathcal{P}$ e $y \in \mathcal{C}$ hay una clave única, $k \in \mathcal{K}$, tal que $E_k(x) = y$*

Ejemplo 22. *El algoritmo $One - time\ Pad$ es conocido por ofrecer secreto perfecto, aunque esto se debatió mucho hasta que Shannon desarrolló el concepto. Hasta entonces se pensaba que no podía atacarse, pero no se tenía la certeza.*

El algoritmo puede aplicarse a vectores de n bits, es decir, $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_2)^n$. Para cada clave $k \in (\mathbb{Z}_2)^n$ se define $E_k(x)$ como la suma de los vectores k y x, obviamente en módulo 2 y siendo $x \in (\mathbb{Z}_2)^n$ el mensaje en plano. Un tercer vector $y \in (\mathbb{Z}_2)^n$ sería el texto cifrado.

$$E_k(x) = (x_1 + k_1, \ldots, x_n + k_n) = (y_1, \ldots, y_n) = y$$

Por las propiedades en $(\mathbb{Z}_2)^n$ el proceso de desencriptación es el mismo que el de encriptación pero utilizando y, además de tener como resultado x. La función de desencriptación, $D_k(x)$, es igual a $E_k(x)$ en este caso

También puede aplicarse a mensajes de longitud n y abecedarios de m letras. Las letras se tratan como números en módulo m, sumando en la encriptación y restando al desencriptar. En este caso $\mathcal{P}$, $\mathcal{C}$ y $\mathcal{K}$ son el abecedario de m letras escogido.

Entropía

En el concepto anterior utilizábamos una clave para cada carácter del texto. Con la entropía nos vamos a centrar en qué sucede si una clave se reutiliza con muchos textos, es decir, una gran cantidad de caracteres. ¿Llegará un momento en el que un criptoanalista pueda atacar al algoritmo utilizando solo texto cifrado?

Definición 30. *Sea $\mathcal{X}$ una variable aleatoria que toma valores de un conjunto finito X. La cantidad*

$$H(\mathcal{X}) = -\sum_{x \in X} P[x] \log_2(P[x])$$

se denomina entropía de $\mathcal{X}$.

Nota 18. *Aunque $\log_2(P[x])$ no está definido si $P[x] = 0$ pensamos que el límite de $P[x] \log_2(P[x])$ cuando $P[x]$ tiende a 0 es 0 y no hay problema. Aún así algunos autores la definen como la suma anterior cuando las probabilidades no son nulas. Cambiar la base del logaritmo en la definición solo produce un cambio por una constante en el valor de la entropía*

Recordando nuestro criptosistema $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ y las variables aleatorias del mismo, P, C y K podemos calcular sus entropías si concemos las distribuciones de probabilidad. Las denotamos $H(X)$, $H(C)$ y $H(K)$.

Pero antes de seguir vamos a enunciar algunas propiedades de la entropía. Sean X e Y variables aleatorias, cumplen lo siguiente:

- Si la distribución de probabilidad de X toma los valores $p_i > 0$, con i entre 1 y n. Entonces $H(X) \leq \log_2(n)$ y la igualdad solo se da si $p_i = 1/n$ para todo i.
- $H(X, Y) \leq H(X) + H(Y)$ y la igualdad solo se da si son independientes. Esta es la entropía conjunta.
- La fórmula
$$H(X|Y) = -\sum_{y} \sum_{x} P[y] P[x|y] \log_2(P[x|y])$$
da la entropía condicional y mide la cantidad de información sobre X que no revela Y.
- $H(X, Y) = H(Y) + H(X|Y)$
- $H(X|Y) \leq H(X)$ y la igualdad solo se da si X e Y son independientes.

Claves espurias y distancia de unicidad

Aplicando estos resultados a nuestro criptosistema $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, obtenemos que

$$H(K|C) = H(K) + H(P) - H(C)$$

este valor es denominado equivocación de claves y mide la cantidad de incertidumbre sobre la clave aunque conozcamos el texto cifrado.

Suponiendo que queremos realizar un ataque solo con texto cifrado nuestro objetivo es descubrir la clave que lo generó. Sin embargo, podemos encontrar varias claves que nos den textos claros válidos y solo una de ellas será la correcta.

Definición 31. *Sea la clave $k \in \mathcal{K}$ tal que nos de un texto plano posible pero que no sea el correcto. Entonces diremos que k es una clave espuria.*

Nuestro objetivo es entonces detectar y evitar estas claves. Para ello empezamos estudiando dos nuevos conceptos relacionados con la entropía: la entropía del lenguaje y su redundancia.

La entropía de un lenguaje natural, L, la denotamos por H_L y nos dice cuanta información de valor tenemos en cada carácter de ese lenguaje. Una primera aproximación sería calcular $H(P)$.

Ejemplo 23. *Si consideramos el inglés como el lenguaje natural L. Tenemos la distribución de probabilidad de P en la Tabla 6 y con ella calculamos que $H_L \approx 4{,}19$.*

La de un lenguaje aleatorio, de 26 caracteres, es igual a $\log_2(26) \approx 4{,}70$.

Pero si estudiamos conjuntos de letras como digramas o trigramas la entropía del lenguaje se hace menor, entonces utilizaremos como variable aleatoria P^n cuya distribución de probabilidad es la de los n-gramas posibles en el lenguaje L.

Definición 32. *Sea L un lenguaje natural:*

- *Se denomina entropía de L al valor*

$$H_L = \lim_{n\to\infty} \frac{H(P^n)}{n}$$

- *Se denomina redundancia de L al valor*

$$R_L = 1 - \frac{H_L}{\log_2(|\mathcal{P}|)}$$

El concepto de redundancia mide la fracción de caracteres del lenguaje que "sobran".

Ejemplo 24. *Si retomamos el cálculo con el inglés, hay estudios que han situado su entropía entre 1 y 1.5, si tomamos el valor intermedio 1.25 esto significa que el inglés tiene una redundancia de 0.75.*

No hay que considerar que 3 de cada 4 letras "sobran" en inglés, sino que a la hora de codificar la información de un texto en inglés podría reducirse su tamaño en tres cuartas partes, utilizando códigos diferentes para n-gramas diferentes.

Retomando la claves espurias, gracias al concepto de redundancia, la equivocación de claves y las propiedades de entropía, Shannon propuso una cota inferior al número de estas.

Teorema 10. *Sea el criptosistema $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ tal que $|\mathcal{P}| = |\mathcal{C}|$ y las claves se escogen con probabilidad equitativa. Sea R_L la redundancia del lenguaje utilizado. Si tenemos un texto cifrado de longitud n, con n lo suficientemente grande, el número esperado de claves espurias, $\bar{s}_n$, cumple:*

$$\bar{s}_n \geq \frac{|\mathcal{K}|}{|\mathcal{P}|^{nR_L}} - 1$$

Nota 19. *Esta cantidad tiende rápidamente a 0 al crecer n. No es acertado utilizarlo para valores pequeños de n por la definición de H_L, que aquí se aproxima por $H(P^n)/n$ al asumir que n lo cogemos suficientemente grande.*

El último concepto que vamos a explicar, distancia de unicidad, es el resultado de toda la teoría de Shannon que hemos expuesto y lo vamos a utilizar para comprobar cuanto texto cifrado sería necesario para evitar claves espurias en el caso de la máquina Enigma.

Definición 33. *El valor n_0 para el cual el número de claves espurias, $\bar{s}_n$, se vuelve 0 se denomina distancia de unicidad. Es decir, es la cantidad de texto cifrado que un oponente necesita para poder computar la clave correcta, y solo esta, sin importar cuanto tiempo lleve.*

Si en el teorema anterior hacemos $\bar{s}_n = 0$ y despejamos la n, que será n_0, conseguimos una expresión para la distancia de unicidad.

$$n_0 \approx \frac{\log_2(|\mathcal{K}|)}{R_L \log_2(|\mathcal{P}|)}$$

Ejemplo 25. *Para aplicarla al caso de la máquina Enigma, tomando como lenguaje el inglés, tenemos que:*

- $|\mathcal{P}| = 26$*, pues el inglés tiene 26 letras.*
- $|\mathcal{K}| = 26^3 \times 26^3 \times 6 \times 2 \times \dfrac{26!}{(6!\,10!\,2^{10})}$*, ya que tiene 3 rotores que se pueden ordenar de 6 maneras diferentes, colocar en 26^3 posiciones iniciales y configurar sus anillos de 26^3 maneras distintas. A esto le añadimos que había 2 reflectores diferentes, B y C, y que normalmente se escogían 10 conexiones que nos dan la última fracción.*
- $R_L = 0{,}75$*, por lo dicho anteriormente.*

$$n_0 \approx \frac{78{,}89}{0{,}75 \times 4{,}7} = 22{,}38$$

Es decir que un mensaje con aproximadamente 22 caracteres generalmente solo habría tenido una clave posible, la verdadera. Si nos limitamos a solo los rotores, sin tablero, anillos u otros reflectores, este número baja a 5 caracteres.

8. Conclusiones

Solicité este tema porque siempre me ha gustado la seguridad y las contraseñas, bases para la criptografía. Además conocía los cifrados históricos como Vigenère, había experimentado con ellos e intentado romperlos por mi cuenta. Ante el trabajo presentado en esta memoria esos ataques no eran más que pequeños juegos.

Con este proyecto he aprendido detalles de la máquina Enigma como la existencia de los anillos y los resultados de Rejewski que ayudaron a ganar una guerra y salvar miles o millones de vidas, unos resultados matemáticos.

En este tema incluso me he sentido motivado a crear varios programas para ayudarme: una máquina Enigma sin tablero de conexiones en C#, que me ayudó a entender el funcionamiento de la máquina del todo; y dos programas Java, para los cálculos necesarios del ataque polaco desde interpretar un conjunto de ochenta claves de sesión hasta encontrar las permutaciones $\mathcal{J}$ y $\mathcal{N}$.

Respecto a la máquina de Turing he podido practicar con varios simuladores para realizar los mismos ataques que él hizo, estar atento a las paradas de la Bomba y valorarlas. Esto me ayudó a entender toda la teoría que tiene detrás.

Finalmente con la teoría Shannon doy solo una muestra del criptoanálisis estadístico que podría realizarse. Cómo detectar cifrados seguros o saber cuando realizar un ataque con texto cifrado, son ejemplos de las cosas que he aprendido. El no conocer esta teoría de antes me anima a leer sobre cifrados más actuales y cómo aseguran que son irrompibles, hasta que un grupo de criptoanalistas prueban que no lo eran tanto.

Referencias

[1] Marian Rejewski: MATHEMATICAL SOLUTION OF THE ENIGMA CIPHER (1982) *Cryptologia, 6:1, 1-18.*

[2] Dimitri Gabbasov: Breaking the Enigma (2015)

[3] Rebecca Bellovin: Cracking the Enigma *Imperial College London.*

[4] Nigel P. Smart: Cryptography made simple (2016), Chapter 8. The Enigma Machine *University of Bristol.*

[5] Jirí Tuma: Permutation groups and the Solution of German Enigma Cipher (2003) *Charles University, Prague, Czech republic.*

[6] A. Ray Miller: THE CRIPTOGRAPHIC MATHEMATICS OF ENIGMA (1995) *Cryptologia, 19:1, 65-80.*

[7] Chris Christensen: The Polish Cipher Bureau's attack on the German Enigma Cipher Machine *Northern Kentucky University.*

[8] S. Armstrong, J. Koby, J. A. Vigil, V. Trujillo: Puzzled: The Underlaying Mathematics of the Enigma (2007) *McCurdy School, New Mexico.*

[9] Lysator: Turing Bombe Simulator y su guía de uso, *www.lysator.liu.se.*

[10] Graham Ellsbury: The turing Bombe, What it was and how it worked *www.ellsbury.com/bombe1.htm.*

[11] Donald W. Davies: EFFECTIVENESS OF THE DIAGONAL BOARD (1999) *Cryptologia, 23:3, 229-239.*

[12] Douglas R. Stinson: Cryptography: theory and Practice (2005) Capítulos 1 y 2 *CRC Press.*

[13] Tony Sale: página web *www.codesandciphers.org.uk.*

[14] Bill Casselman: Marian Rejewski and the first break into Enigma *American Mathematical Society, University of British Columbia, Vancouver, Canada.*

[15] Klaus Pommerening: Permutations and Rejewski's theorem (2008) *Johannes-Gutenberg-Universität.*

[16] Román Ceano: Ultra: Enigma y Fish (2015) *Madrid, XI ciclo conferencias UPM TASSI.*