Contents

1 Contexto criptográfico

Cifrado César

Funcionamiento
Dado un número cualquiera $n \in \{0, ..., 25\}$, el cifrado César de desplazamiento n de una letra, codificada en $\mathbb{Z}_{26}$, se define como

$$E_n(x) := (x + n) \mod 26$$

Vulnerabilidades. ¿Por qué es fácilmente descifrable?

- Únicamente hay 26 formas de encriptación. El análisis de frecuencias es muy sencillo.
- Hay que mandar la clave n.

Distintos algoritmos resolvieron parcialmente estos problemas, pero la Máquina Engima tiene mecanismos para resolver los 2 primeros muy efectivamente, y el último parcialmente.

Cifrado de Vigenère

Funcionamiento
Dada una tupla de números $(c_1, ..., c_r)$, siendo $c_i \in \{0, ..., 25\}$, el cifrado de Vigenère de clave $(c_1, ..., c_r)$ de una frase $x_1x_2 \cdots x_n$, codificada en $\mathbb{Z}_{26}$, se define como

$$E_n(x_1x_2 \cdots x_n) := (x_1 + c_1), \cdots, (x_{r+1} + c_1), \cdots, (x_n + c_{n\%r+1}) \mod 26$$

Ventajas y vulnerabilidades

- Ya hay 27^r formas de encriptación, suficientes para la época.
- Buscando series de grupos de letras que se repitan periódicamente, se puede deducir el número de letras de la clave, y a partir de ahí hacer r análisis de frecuencias.
- Hay que mandar la clave $(c_1, ..., c_r)$.

¿Qué buscaban en una encriptación?
Se desarrollaron diversos métodos, pero si el "enemigo" capturaba a un soldado aliado, podía sacarle la información del encriptado. Tenían 3 problemas principales:

1. Una gran cantidad de formas de encriptación.
2. Evitar el análisis de frecuencias.
3. Aunque se le informe al enemigo de la forma y clave de encriptación, podemos seguir comunicándonos con otros soldados.

Enigma resolvió los 3 problemas.

2 La Máquina Enigma

La Máquina Enigma
Los alemanes crearon una máquina con varios rotores (en este caso 3) que se colocaban y giraban en función de sus necesidades.

Figure 1: Imagen de una Máquina Enigma real.

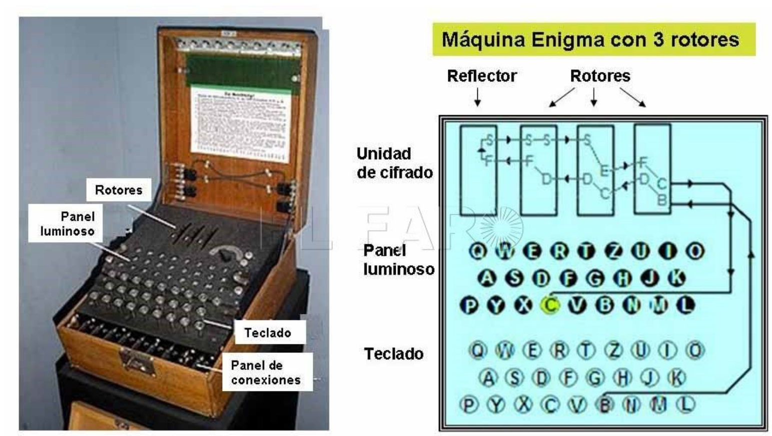
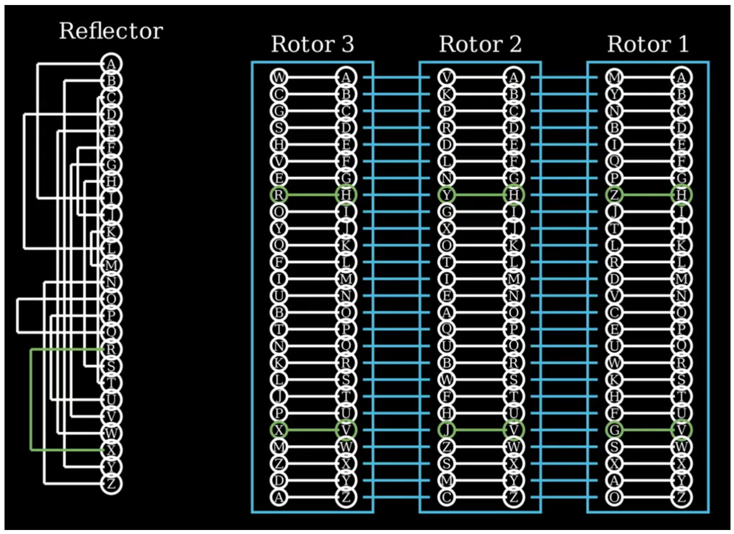


Figure 2: Representación interna de la Máquina Enigma.

La Máquina Engima

Vídeo demostrativo del funcionamiento de la Máquina Enigma



Modelización matemática de Enigma

Características matemáticas de sus componentes

1. Cada rotor internamente realiza siempre la misma permutación. Llamemos a estas permutaciones $\sigma_1, \sigma_2, \sigma_3 : \mathbb{Z}_{26} \to Z_{26}$, en orden de derecha a izquierda.

2. Dada una configuración inicial, en una iteración k, para pasar de un rotor, i, a otro, $i+1$, se está realizando una permutación $p^{(k)}_{i+1\leftarrow i} : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$.

3. Al volver, esta permutación se invierte; $p^{(k)}_{i+1\to i} = (p^{(k)}_{i+1\leftarrow i})^{-1}$.

4. Por último, al llegar al reflejo final, se realiza una permutación $r : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ con la importante propiedad de que, al ser un reflejo, es involutivo, es decir, $r^{-1} = r$. Esta propiedad es muy importante para el descifrado sencillo de mensajes.

Modelización matemática de Enigma

Características matemáticas de sus componentes
Así, en la iteración k, si definimos

$$pasoAIzquierda(x) := \sigma_3 \circ p_{3\leftarrow 2} \circ \sigma_2 \circ p_{2\leftarrow 1} \circ \sigma_1(x)$$

$$pasoADerecha(x) := \sigma_1^{-1} \circ p_{2\rightarrow 1} \circ \sigma_2^{-1} \circ p_{3\rightarrow 2} \circ \sigma_3^{-1}(x)$$

entonces la aplicación de la Máquina a una letra $x \in \mathbb{Z}_{26}$ sería

$$E_k(x) = pasoADerecha \circ r \circ pasoAIzquierda\ (x)$$

Modelización matemática de Enigma

Involución del encriptado de la Máquina Enigma
Proposición. El encriptado Enigma para un mismo paso k es involutivo, i.e., $E_k^{-1} = E_k$.

Demostración. (Posiblemente sería mejor hacerla en pizarra, explicando los pasos)

$$E_k^{-1} = pasoAIzquierda^{-1} \circ r^{-1} \circ pasoADerecha^{-1} =$$

$$= \left(\sigma_1^{-1} \circ p_{2\leftarrow 1}^{-1} \circ \sigma_2^{-1} \circ p_{3\leftarrow 2}^{-1} \circ \sigma_3^{-1}\right) \circ r \circ \left(\sigma_3 \circ p_{3\rightarrow 2}^{-1} \circ \sigma_2 \circ p_{2\rightarrow 1}^{-1} \circ \sigma_1\right) =$$

$$\left(\sigma_1^{-1} \circ p_{2\rightarrow 1} \circ \sigma_2^{-1} \circ p_{3\rightarrow 2} \circ \sigma_3^{-1}\right) \circ r \circ \left(\sigma_3 \circ p_{3\leftarrow 2} \circ \sigma_2 \circ p_{2\leftarrow 1} \circ \sigma_1\right) =$$

$$= pasoADerecha \circ r \circ pasoAIzquierda = E_k$$

Modo de empleo alemán
Sin embargo, los alemanes no podían elegir una configuración y quedarse con ella, pues entonces cualquiera que obtuviera una máquina podría descifrar los mensajes. Lo bueno es que para una máquina, hay $\binom{3}{2}$ ordenes de rotores, y 26 posiciones por rotor, luego hay $6 \cdot 26^3 = 105,456$ configuraciones distintas.

Modo de empleo

1. Al principio de cada mes, se mandaba una libreta con una configuración diaria.

2. El emisario coloca la configuración que toque, y manda 2 veces una terna de letras elegidas, e.g., STGSTG. A continuación inicializa cada rotor con la letra elegida.

3. El receptor lee las 6 primeras letras, coloca los rotores como corresponda, y lee el resto del mensaje.

Modo de empleo alemán

Ventajas

- Inutiliza el análisis de frecuencias.
- Hace falta la libreta mensual para descifrar mensajes.
- Aún si se intercepta un trozo de mensaje y se tiene la libreta, hace falta el inicio del mensaje para entenderlo.
- Una configuración distinta cada día, y en cada mensaje.

Inconvenientes

- No es trivial mandar mensualmente la libreta.
- Mandar 2 veces las mismas letras trae problemas... Lo veremos a continuación.
- Alan Turing no era alemán.
- Hay una película que se llama "Descifrando Enigma", así que algo pasaría.

3 Descifrando Enigma

Problema a resolver

Cuando empezó la guerra, los alemanes, viendo que los polacos estaban realizando progresos, añadieron un proceso de cableado previo, en el que 6 letras del alfabeto original se cambiaban por otras 6 para ser introducidas

Figure 3: Marian Rejewski.

en el primer rotor. De esta forma, había $\binom{26}{12}$ formas de elegir las letras, y $\frac{1}{2^6} \cdot \binom{12}{6} \cdot 6!$ formas de elegir la forma en la que conectamos estas 12 letras.

En total, hay

$$105,456 \cdot \binom{26}{12} \cdot \frac{1}{2^6} \cdot \binom{12}{6} \cdot 6! \sim 10^{16}$$

configuraciones distintas de la máquina. Creando así un sistema inviable de estudiar por ningún método ni remotamente exhaustivo.

Solución de Marian Rejewski

Los polacos consiguieron interceptar algunas máquinas Enigma, y, gracias a un equipo de grandes matemáticos que había allí en la época, consiguieron grandes resultados. En particular, uno de ellos, *Marian Rejewski*, desarrolló un método que permitió la desencriptación de los mensajes alemanes.

Solución de Marian Rejewski

	1st	2nd	3rd	4th	5th	6th
1st message	L	O	K	R	G	M
2nd message	M	V	T	X	Z	E
3rd message	J	K	T	M	P	E
4th message	D	V	Y	P	Z	X

1st letter	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
4th letter	F	Q	H	P	L	W	O	G	B	M	V	R	X	U	Y	C	Z	I	T	N	J	E	A	S	D	K

Rejewski se dio cuenta de que las repeticiones de caracteres entre las 6 primeras letras daban mucha información. Primero ordenaba varios mensajes de la siguiente forma:

Solución de Marian Rejewski

Con esta información, y la de los pares de letras (2, 5), (3, 6), que correspondían, originalmente, a la misma letra, se dio cuenta de que se cumplía una propiedad interesante de las *cadenas de Rejewski* de permutaciones generadas:

Esta propiedad consiste en que la longitud de estas cadenas era constante sin importar el orden del cableado de 6 pares de letras inicial. Así se redujo la cantidad de configuraciones a explorar al mismo que sin cableado; $105,456$ configuraciones. Pero Rejewski tenía un truco más.

Solución de Marian Rejewski

Primero encargó a su equipo que recopilara las cadenas generadas por las $105,456$ posibles configuraciones. Tras un año, las obtuvieron todas, y, viendo el invariante anterior, las catalogaron de acuerdo a esta información de la siguiente forma: Esto es un invariante de la cadena, y además cada cadena tiene una única forma de entre estas. Gracias a todo esto, Rejewski consiguió descifrar Enigma.

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

4 chains from the 1st and 4th letters, with 3, 9, 7 and 7 links.
4 chains from the 2nd and 5th letters, with 2, 3, 9 and 12 links.
5 chains from the 3rd and 6th letters, with 5, 5, 5, 3 and 8 links.

Solución de Marian Rejewski

Primera solución de Enigma

1. Rejewski recopilaba mensajes del día hasta obtener las cadenas correspondientes a las primeras letras.

2. A partir de este invariante, descubría la estructura de rotores que tenían las máquinas ese día en particular.

3. Con los rotores en posición, el juego era trivial, pues estaban todas las letras, menos 12, colocadas correctamente, luego se buscaban frases como *alliveinbelrin*, que se suponía que significaba *arrie in Berlin*, por lo que se sustituía la *r* por la *l* en el cableado, y se proseguía hasta terminar.

4 Codificación teórica mediante la Máquina de Turing

- different themes
- different themes
- different themes
- different themes

Muchas gracias por escuchar !

Joaquín Mateos Barroso [1em] i22mabaj@uco.es