Máquina Enigma y Máquina de Turing

Cómo el análisis combinatorio salvó miles de vidas y Alan Turing creó el marco teórico para la codificación en ordenador

Joaquín Mateos Barroso

i22mabaj@uco.es
Códigos y Criptografía
Profesor: Jónatan Herrera Fernández
4^o Ingeniería Informática
Universidad de Córdoba

October 26, 2024

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 $x_1 x_2 \cdots x_n$, codificada en $\mathbb{Z}_{26}$, se define como

$$E_n(x_1 x_2 \cdots x_n) := (x_1 + c_1), \cdots, (x_{r+1} + c_1), \cdots, (x_n + c_{n\%r+1}) \mod 26$$

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.

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.

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.

La Máquina Engima

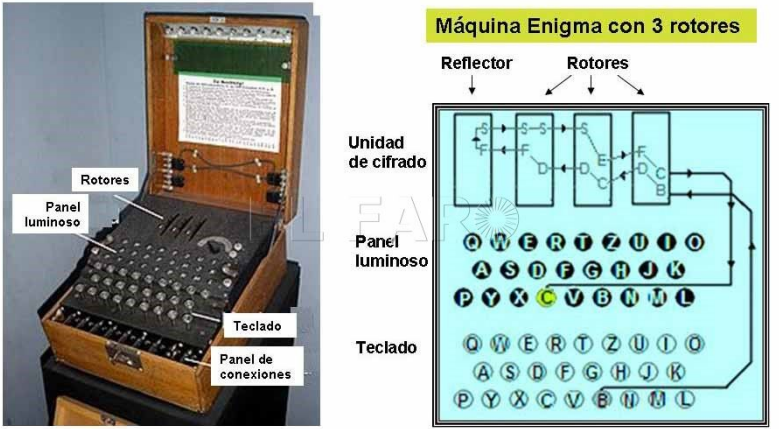
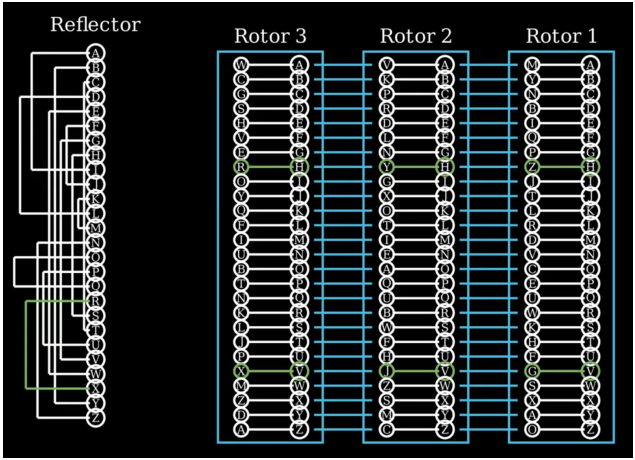


Figure 2: Representación interna de la Máquina Enigma.

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 $\sigma_1, \sigma_2, \sigma_3 : \mathbb{Z}_{26} \to Z_{26}$.
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; $p^{(k)}_{i+1\to i} = (p^{(k)}_{i+\leftarrow i})^{-1}$.
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 fue muy importante para el descifrado sencillo de mensajes.

Modelización matemática de Enigma

Así, en la iteración k, si definimos

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

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

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

Title

- different themes which are usable in practice

Figures

Figure 3: Logo of the university.

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

Thank you for listening !

Joaquín Mateos Barroso

i22mabaj@uco.es