

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO



Facultad de Ingeniería



Práctica 5.

Máquina Enigma

Asignatura: Criptografía

Grupo: 02

Integrantes del equipo:

- Carandia Lorenzo Brenda Fernanda
- Cuadriello Valdés Cynthia Citlalli
- Cuadriello Valdés Diana Sinsuni
- Jose Laguna Daniel
- López Sugahara Ernesto Danjiro
- Rodríguez Kobeh Santiago

Semestre 2026-1

Fecha de entrega de 4 de septiembre de 2025

OBJETIVO

Realizar la explicación, en forma de una investigación, del funcionamiento mecánico y conceptual de la máquina Enigma.

DESARROLLO

Contexto Histórico

Arthur Scherbius, ingeniero e inventor alemán, construyó en los años 20 'Enigma', un aparato electromecánico de rotores para codificar mensajes, con la idea de que la utilizaran bancos y empresas comerciales para mantener en secreto sus comunicaciones. En principio no tuvo un éxito comercial importante, pero cuando Hitler rearmó Alemania en los años 30, se convirtió, con varias mejoras y modificaciones, en la máquina de cifrado estándar de los tres ejércitos alemanes, que basaban en ella la seguridad de sus comunicaciones por radio y que llegó a ser la más avanzada de su época. La dificultad extrema de descifrar su código era una pesadilla para los servicios secretos aliados y aseguraba una enorme ventaja militar al III Reich.

Para que dos operadores de Enigma se comunicaran, las dos máquinas tenían que estar configuradas exactamente igual. Los mensajes, una vez codificados, se enviaban por radio utilizando el código Morse. Quien interceptara estos mensajes, sólo obtenía una serie de letras sin sentido. Sin embargo, un operador de Enigma con las claves adecuadas, al teclear esas series sin sentido, haría que se iluminaran en el panel de lámparas las letras del mensaje original y obtendría el mensaje descodificado. La configuración de la máquina se cambiaba diariamente, de manera que aunque se descifrara el código un día, al día siguiente había que empezar de cero nuevamente.

Partes de la máquina Enigma

Con una apariencia similar a la de una máquina de escribir, Enigma estaba compuesta por cuatro partes principales:

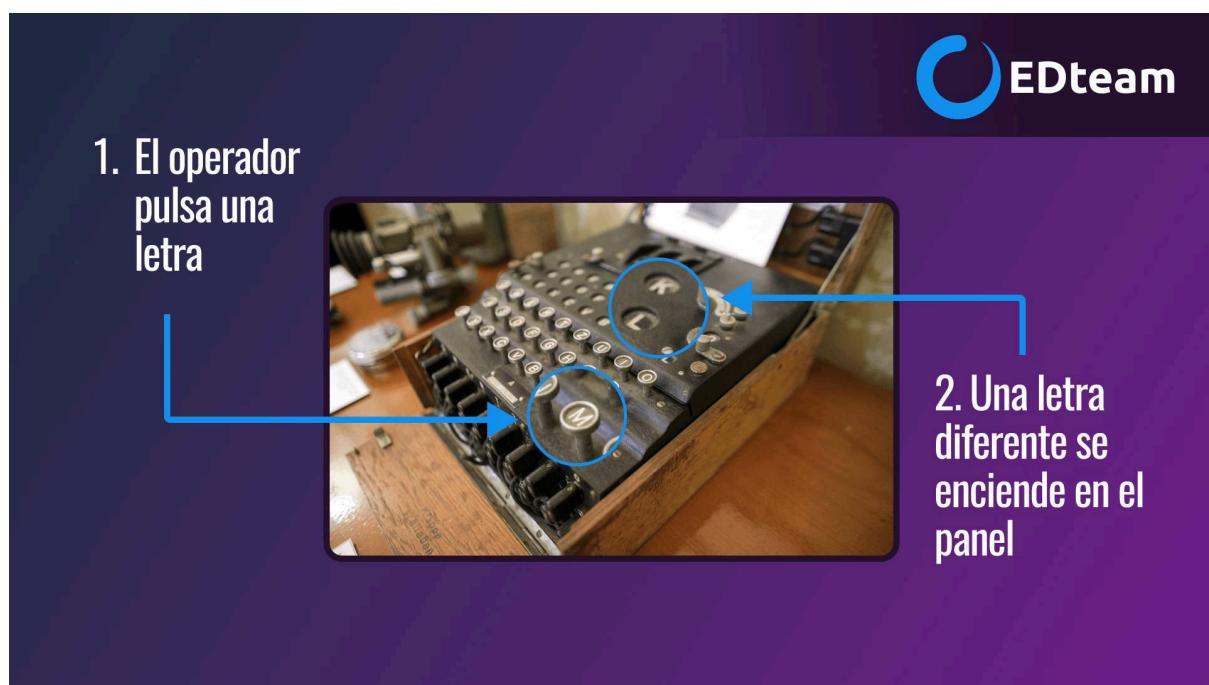
- Teclado: En él se escribían el texto en claro (mensaje a encriptar) y el criptograma (mensaje encriptado) para convertir uno en el otro y viceversa.
- Panel de lámparas: Es aquí donde se indica la letra por la que se codifica la introducida en el teclado.
- Mecanismo de cifrado: Es el corazón de la máquina, ya que es en él donde se produce el proceso de cifrado, y está compuesto por tres rotores y un reflector. Tanto un rotor como un reflector son un disco con 26 posiciones

(cada una de las letras del alfabeto) con conexiones internas entre ellas, pero tienen nombres distintos ya que existen diferencias en su estructura y principalmente en su funcionamiento. Para aumentar la seguridad, existían varios reflectores y rotores diferentes (distintas conexiones internas).

- Clavijero: En él aparecen las letras del alfabeto, que se pueden conectar entre sí mediante cables para intercambiarlas antes de que el mecanismo de cifrado las codifique.

¿Cómo funcionaba Enigma?

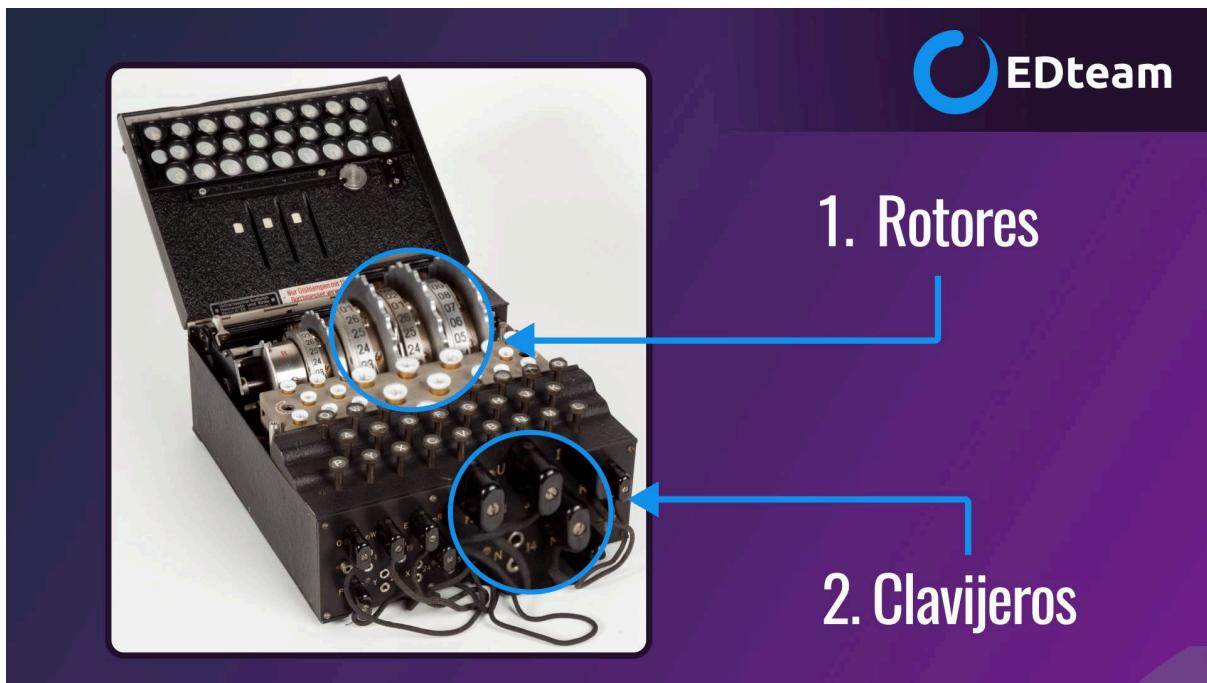
En sencillo, la máquina Enigma remplazaba una letra por otra, así de fácil. El operador pulsaba una letra en el teclado y otra se iluminaba en el panel.



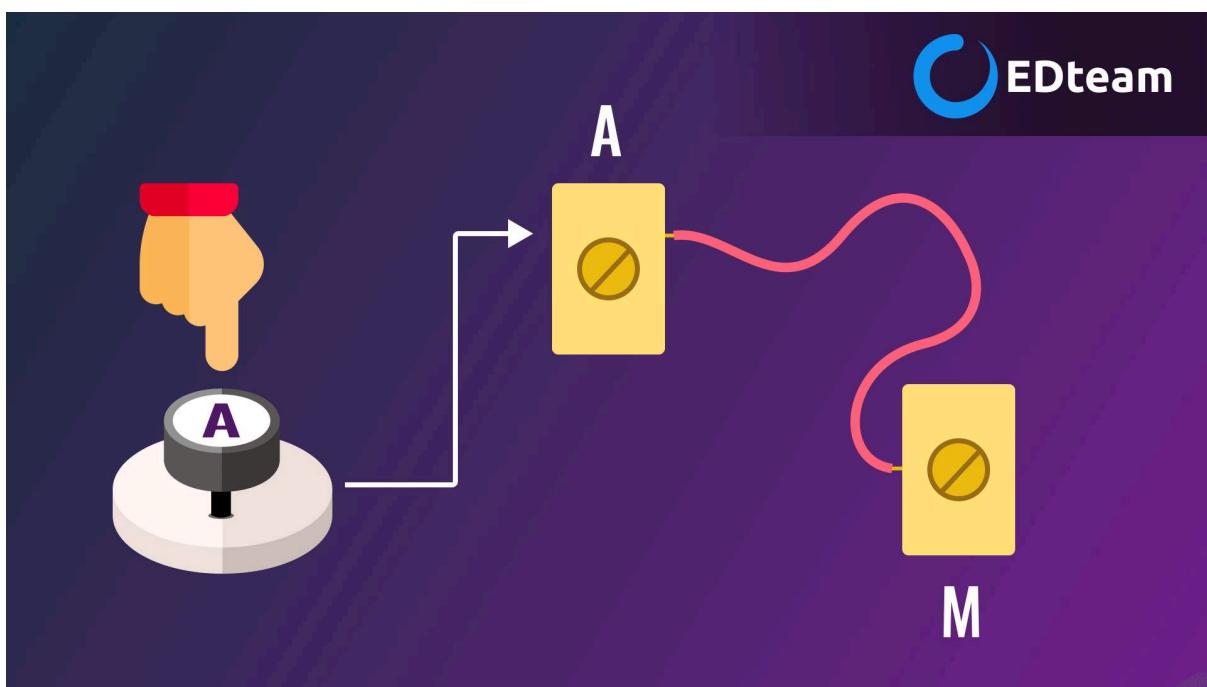
Lo complejo era que tenía cientos de miles de millones de combinaciones posibles. Así es como funcionaba:

Enigma tenía tres rotores que cambiaban una letra por otra. Antes de empezar a cifrar un mensaje el operador giraba los rotores a una posición determinada.

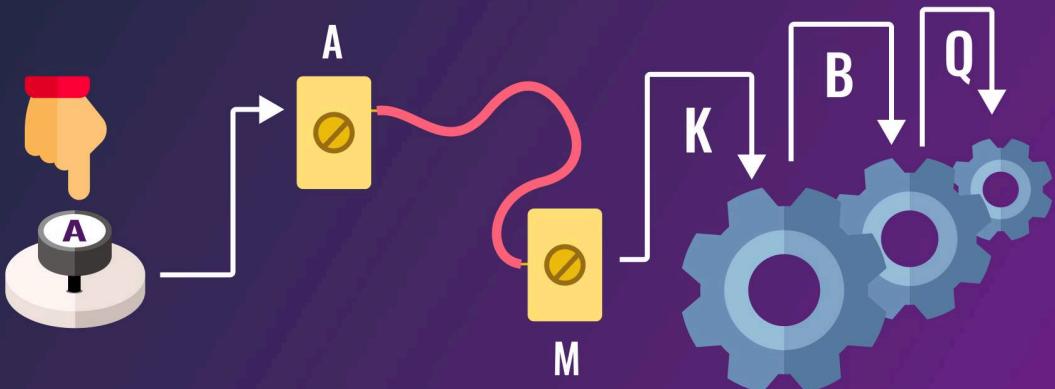
Además tenía unos clavijeros que formaban parejas de letras para reemplazarlas.



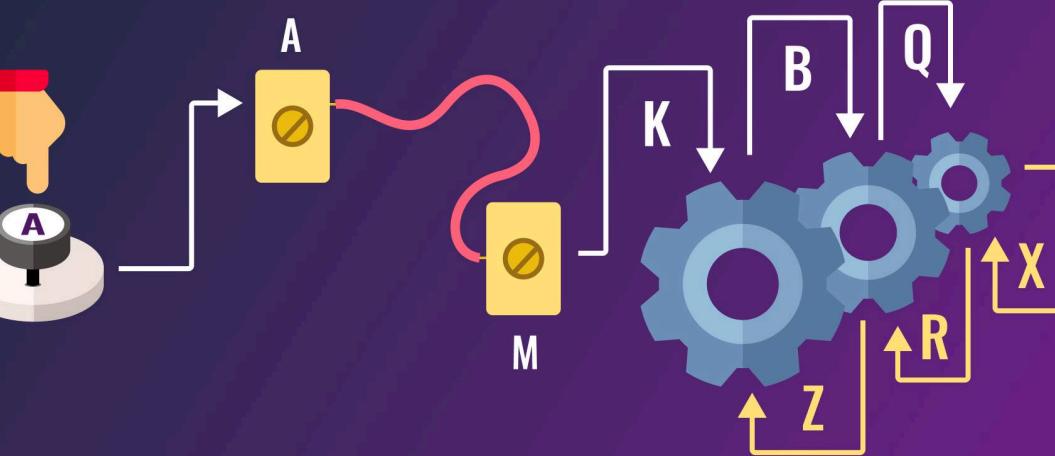
Entonces, cuando un operador pulsaba una letra en el teclado, ésta se transformaba por otra en el clavijero.



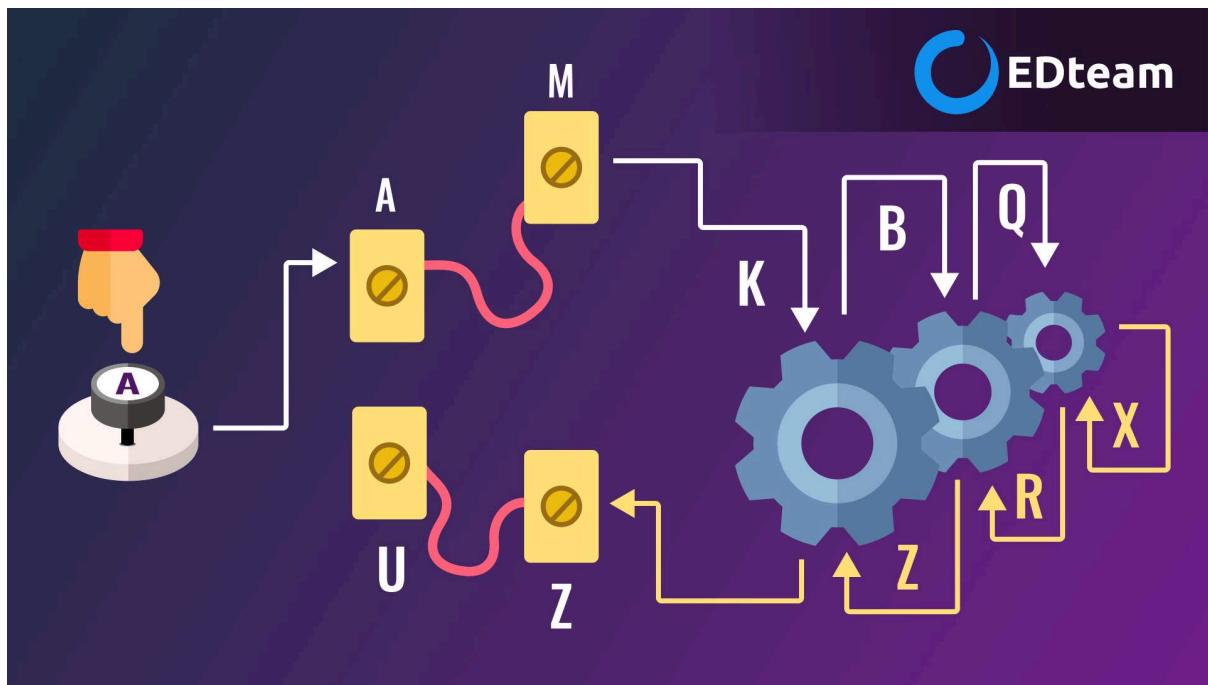
Luego se transformaba por otra en el primer rotor, por otra en el segundo rotor y por otra en el tercer rotor. Cada vez que un rotor cambiaba una letra, también cambiaba de posición, cambiando toda la configuración de la máquina.



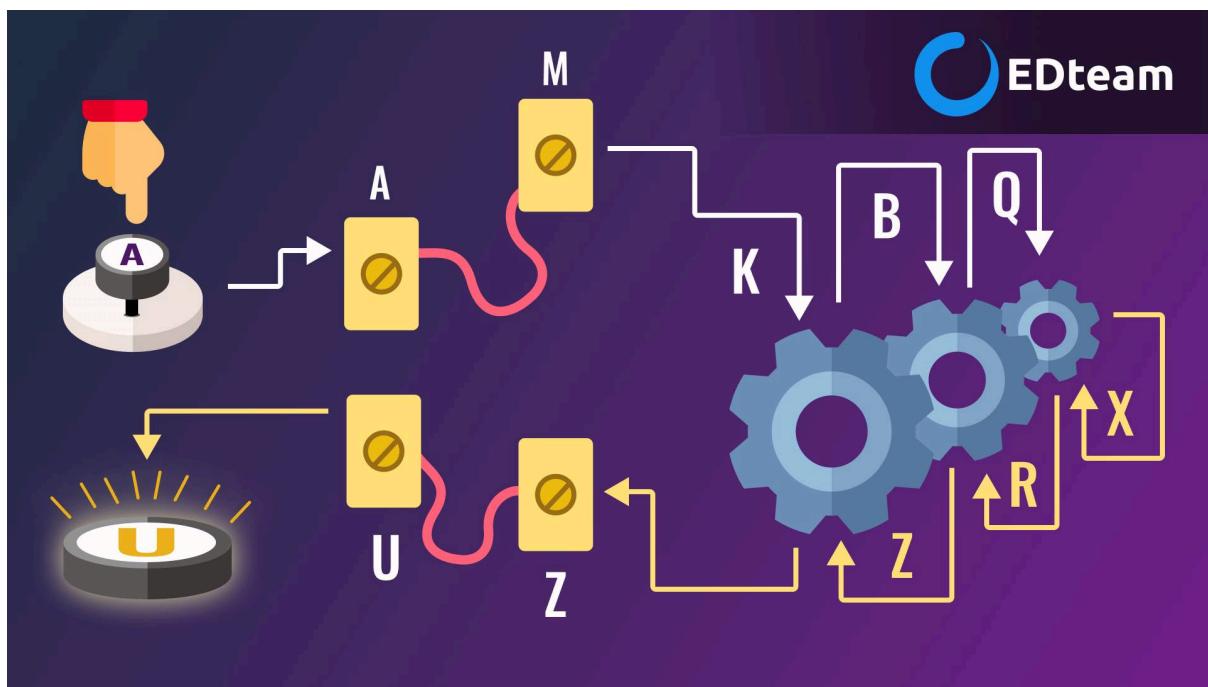
Después se hacía todo el proceso al revés. Primero los rotores (que volvían a cambiar de posición cada vez que cambiaban una letra).



Luego los clavijeros:



Y el resultado se iluminaba en el panel.



El operario de la máquina iba anotando cada letra iluminada y una vez que tenía el mensaje resultante, lo enviaba por código morse al receptor, que hacía el proceso a la inversa: introducía el mensaje cifrado en Enigma y en el panel de luces aparecían las letras del mensaje.

Por lo tanto, el hecho de que al teclear un mensaje se obtuviera un criptograma u otro dependerá de la configuración inicial de la máquina: conexiones en el clavijero,

qué rotores se usan, en qué orden, cuál es su posición inicial, y qué reflector se usa. Esta configuración era conocida como la *clave de la máquina*.

¿Cómo se descifró Enigma?

Para descifrar Enigma se necesitaba saber la posición de los rotores y de los clavijeros. Y considerando la cantidad de combinaciones posibles, ir probando una por una no era una opción (los operadores nazis sabían las posiciones porque recibían las instrucciones al inicio de cada mes).

Así que los codebreakers analizaban los mensajes para encontrar palabras que tenían mucha probabilidad de aparecer (como Hail Hitler). Y puesto que una letra nunca se cifraba como sí misma, podían buscar manualmente si existían repeticiones para descartar esa opción o aceptar esa opción.

Por ejemplo, si suponemos que se ha cifrado EDteam por XAMXQJ podemos descartar esa opción porque la misma letra E que se repite en el mensaje original, se repite también en el mensaje cifrado.



Pero aun así, el avance era muy lento y eran pocos los mensajes que podían descifrarse, así que Turing diseñó una máquina llamada Bombe, inspirada en otra máquina que habían creado antes los polacos para descifrar una versión menos segura de Enigma.

Y puesto que Enigma se descifraba con la misma Enigma, la Bombe de Turing era una réplica de 36 máquinas Enigma con sus rotores y clavijeros. A esta máquina se le introducían las configuraciones que se suponía que debería tener la máquina y ésta descartaba la opción si encontraba colisiones o letras repetidas.

REFERENCIAS

ED Team (2023). *Alan Turing: El genio que descifró el código nazi e inventó la computadora.* Recuperado el 07 de septiembre de 2025, de

[https://ed.team/blog/alan-turing-el-genio-que-descifro-el-codigo-nazi-e-inve
nto-la-computadora](https://ed.team/blog/alan-turing-el-genio-que-descifro-el-codigo-nazi-e-invento-la-computadora)

Macheño Roa, P. (2021). *Una Breve Aproximación al Código Nazi: Enigma.*

Recuperado el 07 de septiembre de 2025, de
<https://qed.mat.uam.es/revista/articulo/enigma>