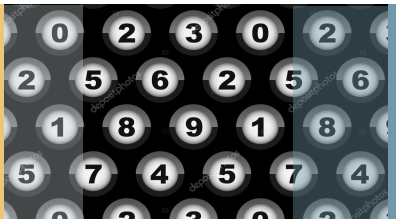
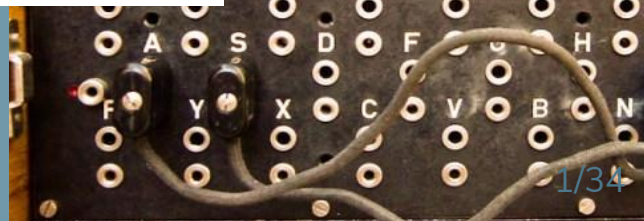
Criptografía y Computación

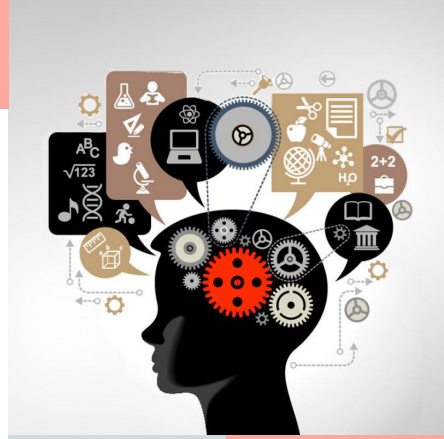
ENIGMA

Ana Puertas Olea
Gema Correa Fernández





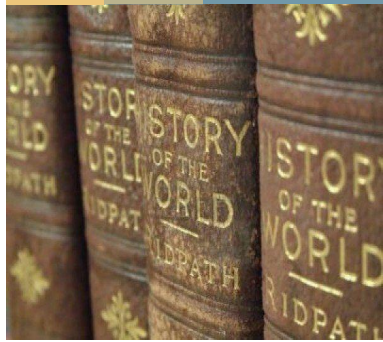
Contenido



1. Contexto Histórico
2. Componentes y Funcionamiento de Enigma
3. Descifrado de Enigma (*Bletchley Park*)
4. Descifrando Enigma (*The Imitation Game*)
5. Bibliografía

CONTEXTO HISTÓRICO

Orígenes, Historia y Versiones de Enigma

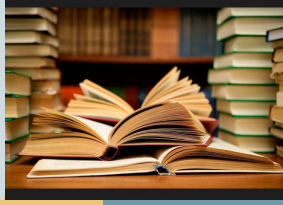


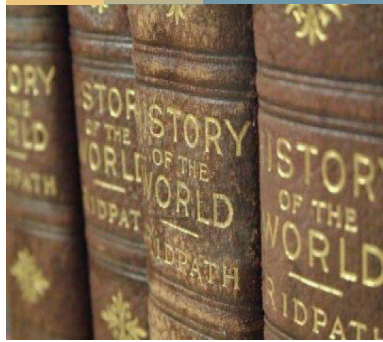
Orígenes

- En el **siglo XX** se produjo la aparición de **máquinas de cifrado con rotores**.
- Una de las que tuvo más repercusión fue la máquina alemana **Enigma**.
- Enigma fue creada por un ingeniero alemán, **Arthur Scherbius**. Esta máquina podía tanto cifrar como descifrar mensajes.
- Su fama se debió al **uso** que hicieron de ella las **fuerzas militares de Alemania en la 2ª Guerra Mundial**.

Historia (I)

- Surgió tras la 1ª Guerra Mundial, cuando su creador, quiso **mejorar los sistemas de criptografía de los ejércitos**.
- Su **idea**, patentada en febrero de 1918, consistía en aplicar el Cifrado de Vigenère, es decir, **aplicar un algoritmo de sustitución de unas letras por otras**.
- Fue creada con el fin de **transmitir secretos comerciales** en el mundo empresarial.



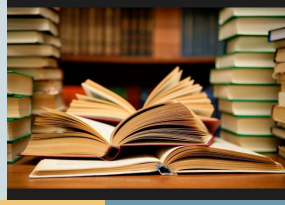


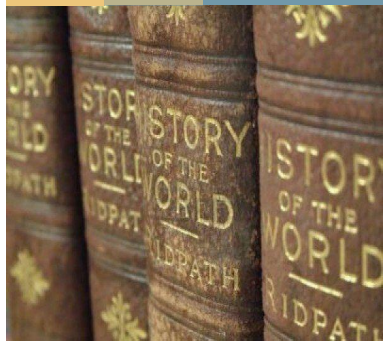
Historia (II)

- Su **fácil utilización**, ya que se parecía a una máquina de escribir, y la **seguridad** que suponía el **cifrado** con ella, fueron las principales razones para su amplio uso (*tanto civil como militar*).

- Esto hizo que la **armada y el ejército alemán**, adquirieran su propia máquina Enigma, adaptándola a sus necesidades, con el fin de aumentar las posibilidades de cifrado y dificultar su criptoanálisis.

- Finalmente, su **sistema de cifrado fue descubierto** y los mensajes desencriptados, hecho que es considerado como una de las causas del desenlace de la 2ª Guerra Mundial.

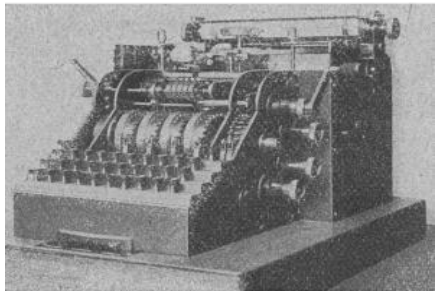


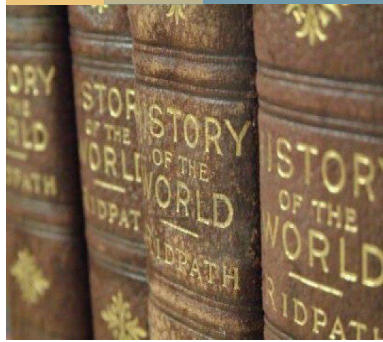


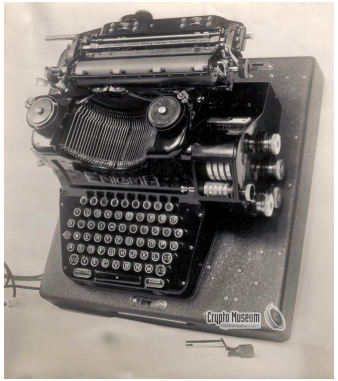
Versiones de Enigma (I)

ENIGMA A (1923)

Fue la primera versión comercial de Enigma.







ENIGMA B (1924)

Fue desarrollada como una mejora de Enigma A.

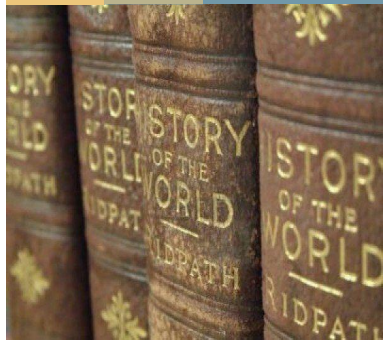
Versiones de Enigma (II)

ENIGMA C (1926)

Se caracterizó por su ligero peso que la hizo más portátil que sus predecesores.

ENIGMA D (1927)

Este modelo se convirtió en el más relevante, siendo utilizado por varios países. Además, fue de gran importancia para los ejércitos alemanes.



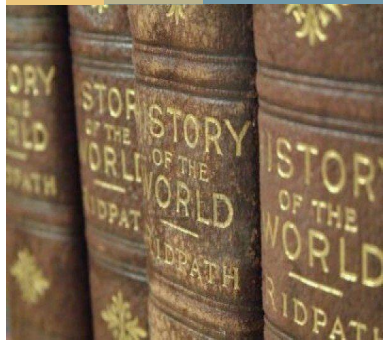
Versiones de Enigma (III)

ENIGMA H (1929)

Sucesor de Enigma B y utilizada principalmente por las fuerzas armadas alemanas.

TYPEX

Máquina utilizada por las fuerzas británicas durante la 2° Guerra Mundial, se trataba de una versión mejorada y reforzada de Enigma.



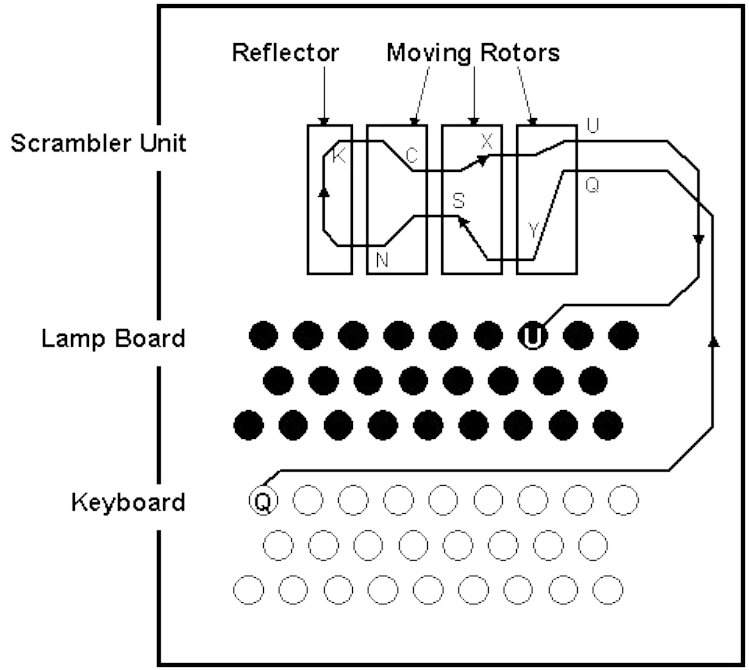
LA MÁQUINA

Componentes y Funcionamiento de Enigma

Componentes y Diseño de Enigma

Partes Mecánicas y Eléctricas

- Teclado Mecánico
- Panel Luminoso
- 3 Rotores
- Reflector
- Batería
- Clavijero



Componentes (I)

TECLADO

Teclado mecánico compuesto por 26 teclas. Cada pulsación de una tecla produce un efecto mecánico en la máquina.

PANEL LUMINOSO

Panel con 26 letras retroiluminadas por bombillas.

Componentes (II)

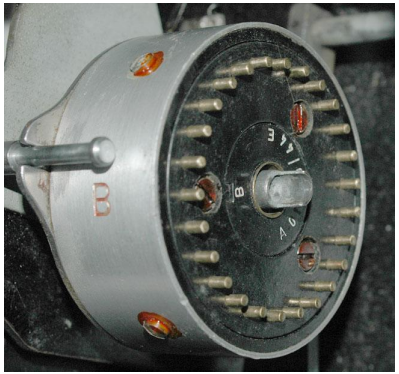
PANEL DE CLAVIJAS

Conjunto de 26 letras que podían ser puenteadas por medio de unos cables (venían diez con cada máquina) que servían para puentear una letra con otra. Con todo esto, se garantiza que una letra no puede ser cifrada como sí misma.

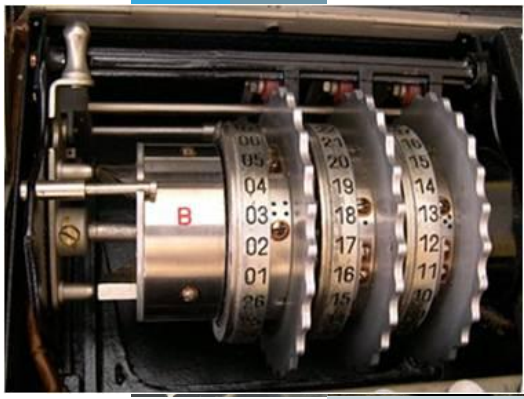
REFLECTOR

Cableado fijo que hace *reflejarse* la señal de nuevo por los rotores, lo que permite un cifrado y descifrado (*el reflector A es el usado en el modelo comercial*).

Cada vez que se pulsa una tecla, la letra cifrada se iluminaba en el panel, con lo que era usual que trabajaran dos operadores para evitar errores y agilizar el trabajo.



Componentes (III)



ROTORES

El código a usar se fijaba con las posiciones de los rotores.

El tercer rotor giraba un veintiseisavo de vuelta después de cada pulsación.

La posición de las conexiones iba cambiando
con cada entrada del teclado → Cifrado Polialfabético

El segundo rotor sólo daba un giro cuando el tercero había completado 26 giros.
El primero cuando el segundo había dado sus correspondientes 26.

Los rotores podían ser intercambiados de posición.La combinación de los tres rotores da una cifra posible de *17.576 cifras* (*26 x 26 x 26*); es decir, que si un mensaje tuviera más de *17.576* letras, aparecerían repeticiones.

Funcionamiento (I)

- La transformación de Enigma para cada letra ⇒ producto de permutaciones
- Si consideramos una máquina Enigma con 3 rotores (3 rotores de los 5 posibles) y un tablero con 10 cables, obtendríamos:

$$\frac{5!}{(5-3)!} = 60 \ combinaciones$$

- Para cada rotor, la posición relativa del cableado al resto del rotor se puede ajustar a 26 posiciones ⇒ $26^3 = 17{,}576$ combinaciones.

Funcionamiento (II)

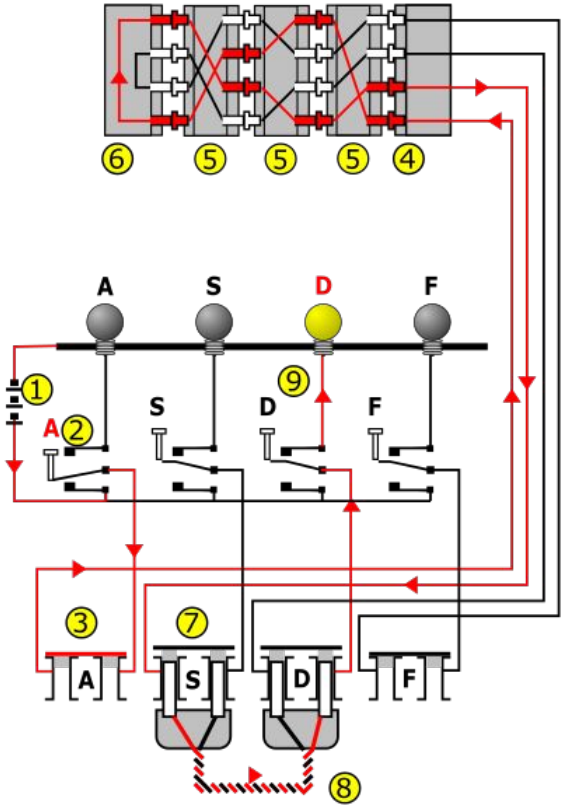
- Cada una de las 20 extremidades de los 10 alambres pueden ser enchufados en cualquiera de las 26 posiciones no ocupadas:

$$\frac{26!}{(26-20)!\cdot 2^{10}\cdot 10!} = 150.738.274.937.250$$

- Por lo tanto, existen ➡ *158,962,555,217,826,360,000 posibles combinaciones*

$$\frac{5!}{(5-3)!}\cdot 26^{3}\cdot \frac{26!}{(26-20)!\cdot 2^{10}\cdot 10!} = 158.962.555.217.826.360.000$$

Funcionamiento (III)



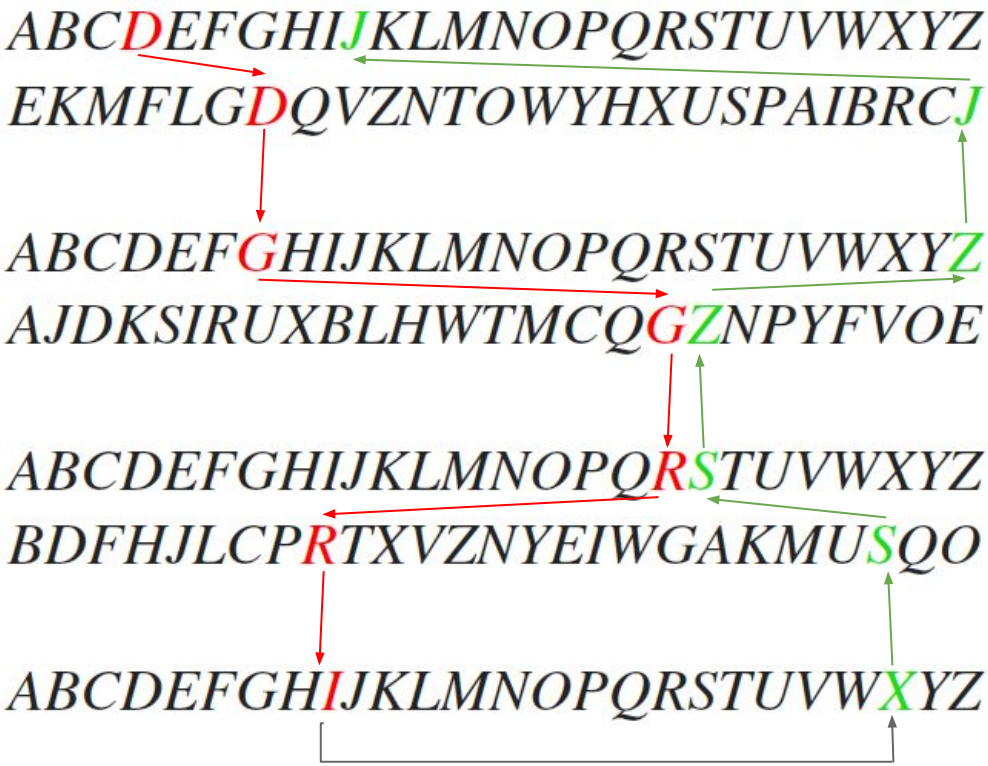
La corriente fluye desde la batería (1) a través de un conmutador de teclado bidireccional (2) presionado hasta el tablero (3).

A continuación, pasa a través de la rueda de entrada (4), pasa por los rotores (5) y entra en el reflector (6).

El reflector devuelve la corriente a través de los rotores (5) y la rueda de entrada (4), a través de un recorrido completamente diferente, pasando por la clavija "S" (7) conectado con un cable (8) a la clavija "D" y otro bidireccional (9) para encender la lámpara apropiada.

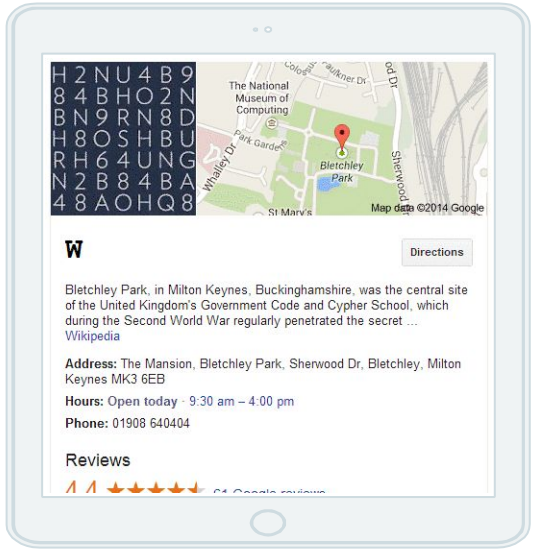
Ejemplo

Rotor	ABCDEFGHIJKLMNOPQRSTUVWXYZ
I	EKMFLGDQVZNTOWYHXUSPAIBRCJ
II	AJDKSIRUXBLHWTMCQGZNPYFVOE
III	BDFHJLCPRTXVZNYEIWGAKMUSQO



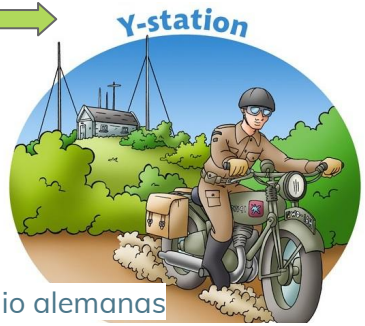
DESCIFRADO DE ENIGMA

Bletchley Park



Un oficial alemán transmite un mensaje cifrado

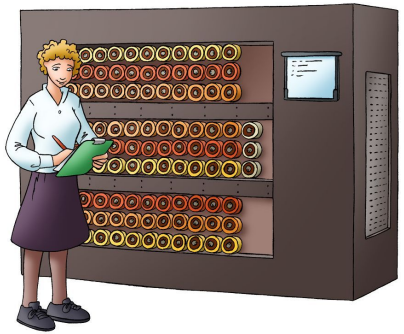
Soldados alemanes del campo de batalla están recibiendo el mensaje y descifrándolo en una máquina Enigma



Las señales de radio alemanas son interceptadas en estaciones secretas y enviadas a Bletchley Park

Se está realizando el trabajo de descifrado (Criptoanálisis)

El Criptoanálisis está siendo probado en las bombas, cuyos resultados son devueltos



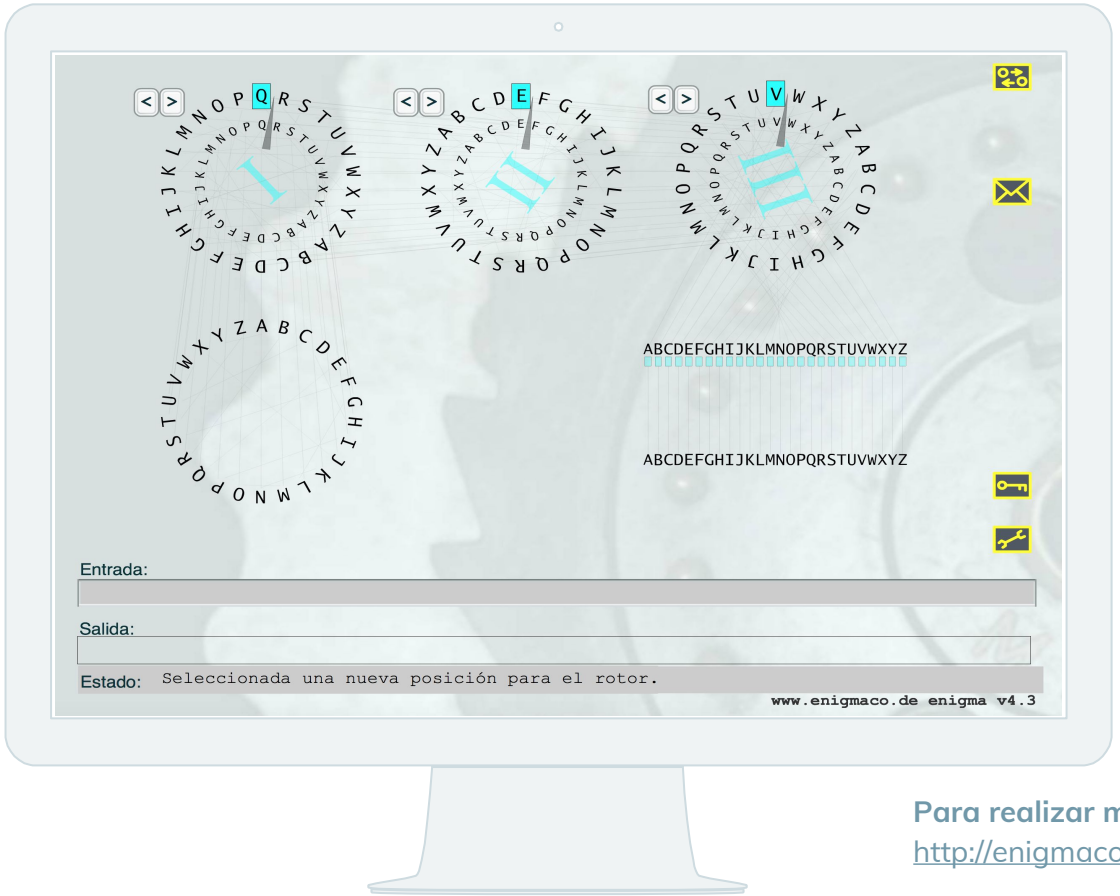
Los descifrados son traducidos y escritos de forma adecuada para las autoridades

¿Cómo desciframos una letra? Ejemplo

- Para poder descifrar una letra o una palabra, tenemos que introducir la misma posición inicial de los rotores y el mismo tipo de reflector usado para cifrar la letra.

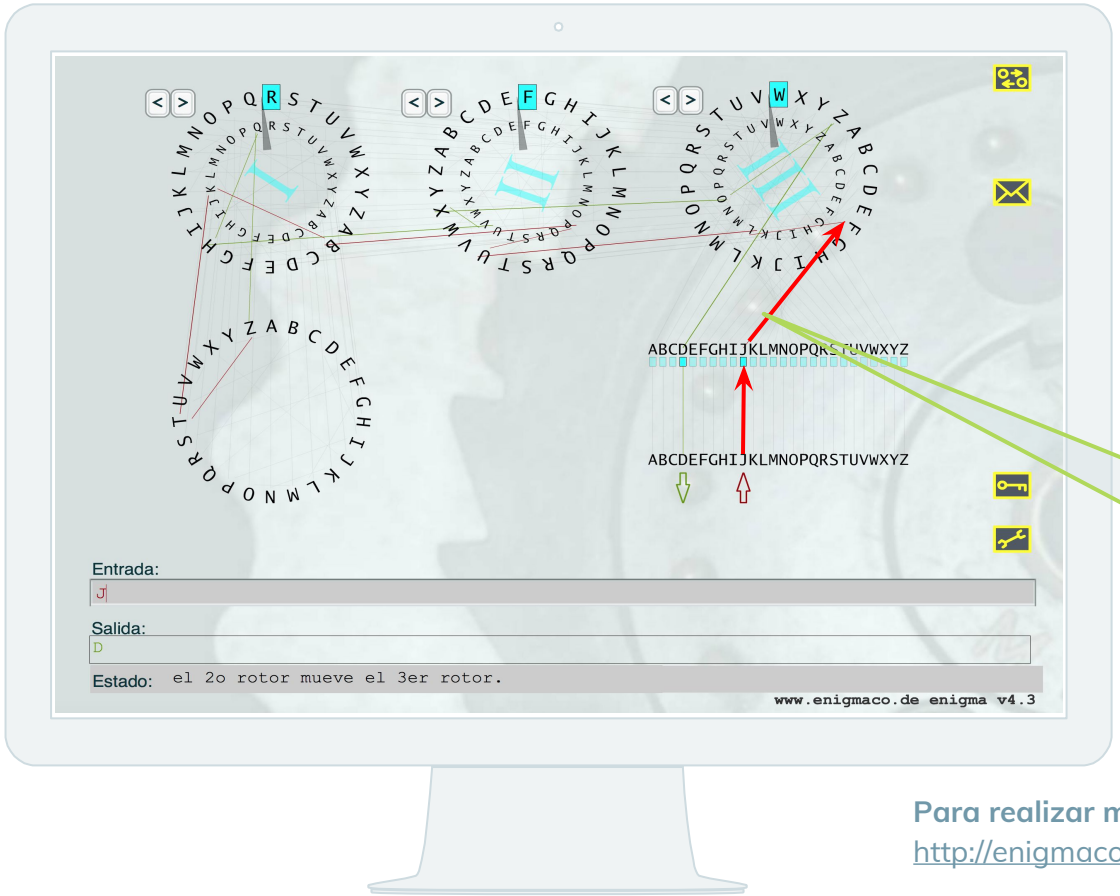
- Probaremos con el siguiente **ejemplo**:
  - Tenemos la misma posición inicial de los rotores que antes *QEV*, pero esta vez vamos a comprobar que la letra cifrada *J*, corresponde a la letra original *D*.

Posición Inicial de los Rotores: **Q E V** Letra Cifrada: **J** Letra Original: **D**



Para realizar más simulaciones
http://enigmaco.de/enigma/enigma_es.html

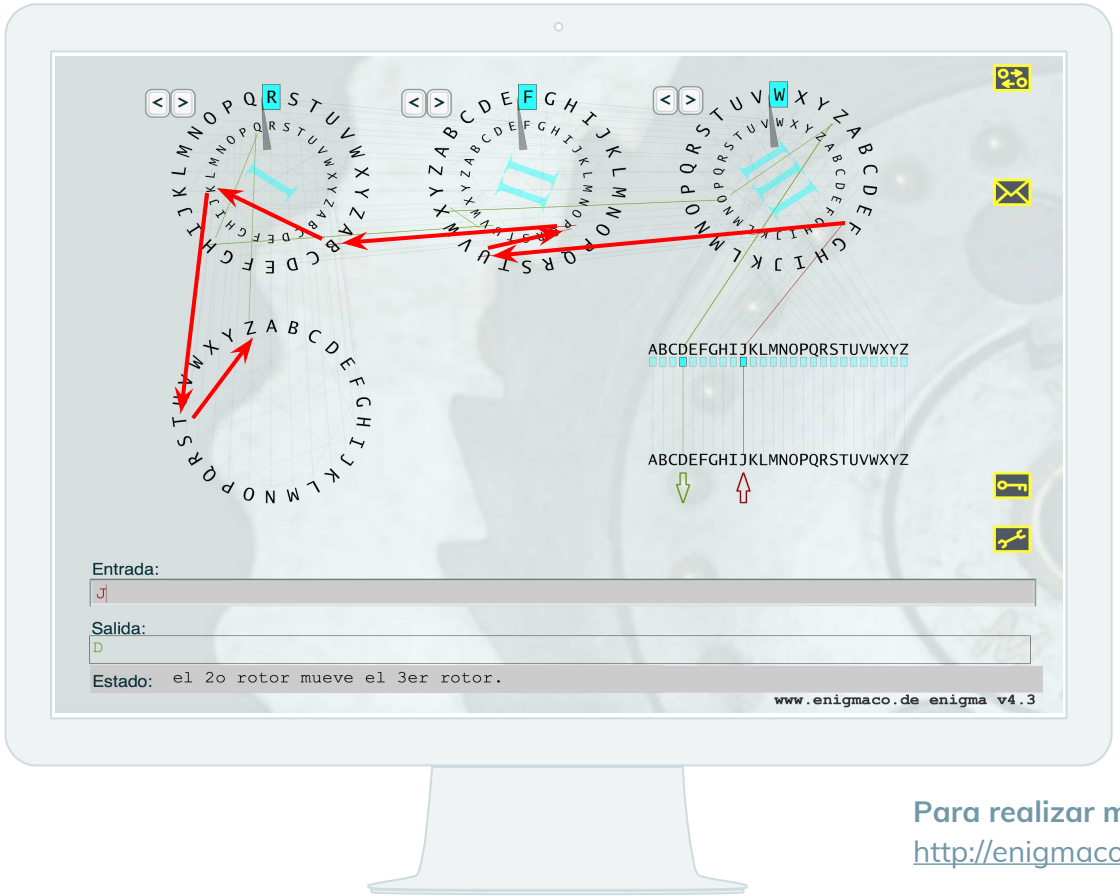
Posición Inicial de los Rotores: **Q E V** Letra Cifrada: **J** Letra Descifrada: **D**



Obtenemos la posición de esa letra en el nuevo alfabeto (Rotor III)

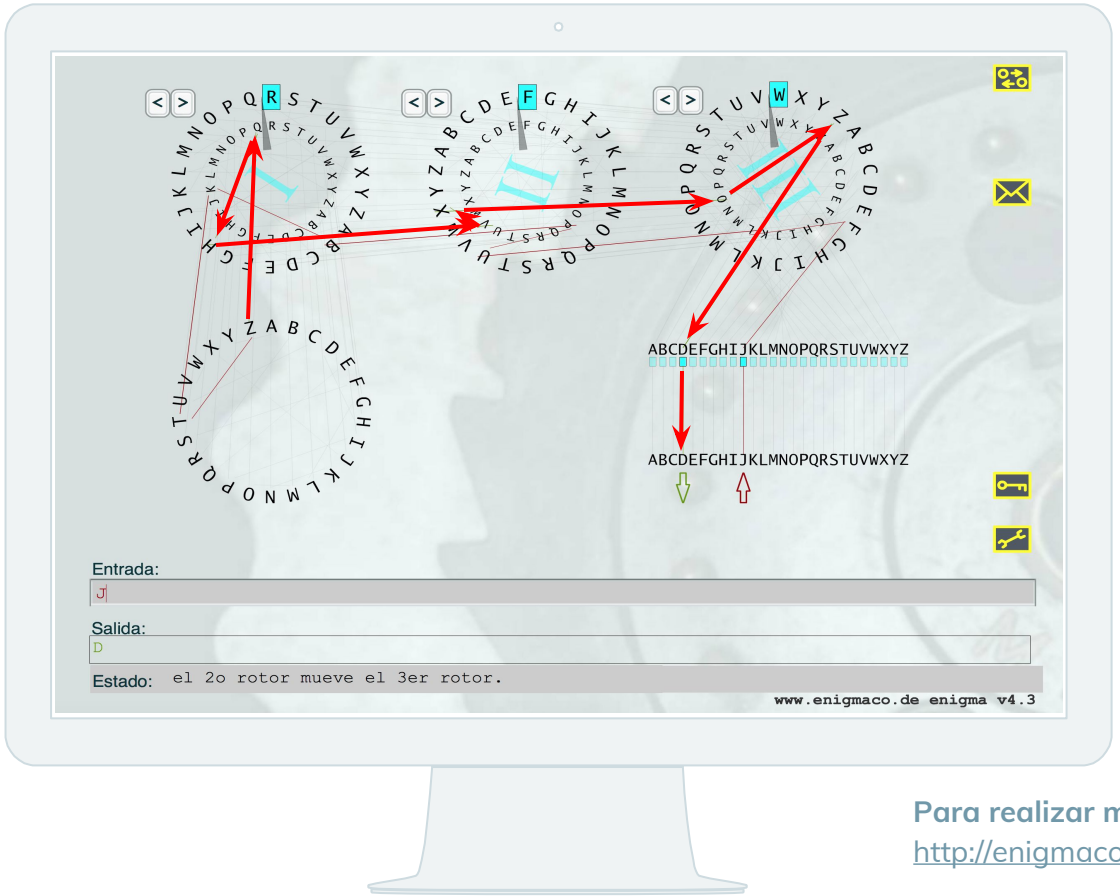
Para realizar más simulaciones
http://enigmaco.de/enigma/enigma_es.html

Posición Inicial de los Rotores: **Q E V** Letra Cifrada: **J** Letra Descifrada: **D**



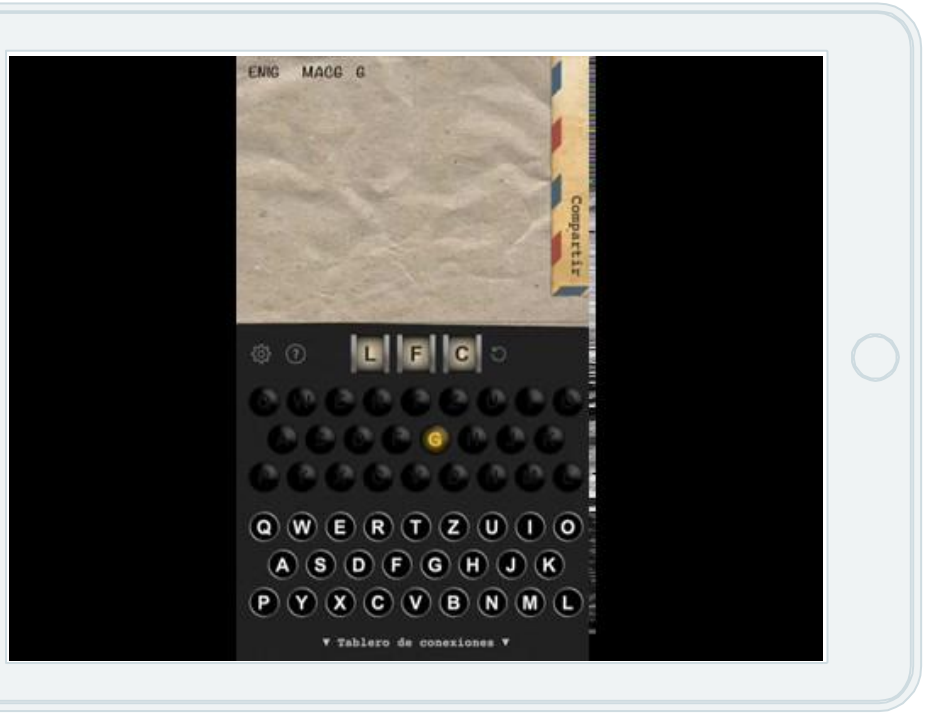
Para realizar más simulaciones
http://enigmaco.de/enigma/enigma_es.html

Posición Inicial de los Rotores: **Q E V** Letra Cifrada: **J** Letra Descifrada: **D**

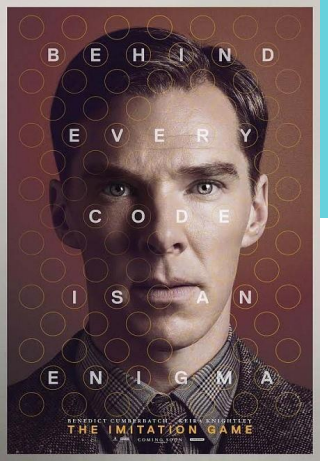


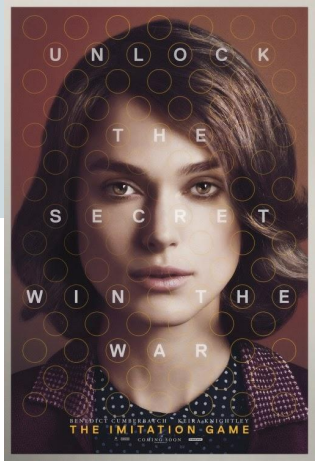
Para realizar más simulaciones
http://enigmaco.de/enigma/enigma_es.html

Descifrando un Mensaje



App Store: **Enigma Cipher**





DESCIFRANDO ENIGMA

The Imitation Game


THE IMITATION GAME

Descifrando Enigma (I)

La máquina fue vencida debido a varios factores:

- Al ser un **modelo comercial muy vendido**, su distribución llegó a gran parte del mundo, por lo que el **principio de funcionamiento ya era conocido**.

- La **inteligencia polaca** llevaba años intentando descifrar Enigma, por eso fue la **primera** en **conseguirlo,** creando para ello máquinas capaces de romper este cifrado.

- Los británicos al igual, intentaron descifrar los códigos alemanes, pero estos ya habían complicado demasiado su cifrado, por lo que no tuvieron tanto éxito.

Descifrando Enigma (II)

- En 1939 una **delegación polaca** explicó sus **hallazgos** sobre Enigma a **los servicios de inteligencia británicos**. Entregando toda la información que habían recogido sobre el descifrado de Enigma y proporcionando unas **bombas criptológicas**, que eran unas máquinas Enigma de procesamiento en paralelo que buscaban las codificaciones posibles.

- Los británicos decidieron trabajar en ello en su centro de **Bletchley Park**, lugar donde finalmente se acabó **descifrando el código** por completo, con la inestimable **ayuda** de **Alan Turing**.

Descifrando Enigma (III)

- El 9 de mayo de 1941, la **Marina Real Británica capturó** un **submarino alemán** donde pudo hacerse con una máquina Enigma y con el preciado **libro de claves**. Esta captura se mantuvo en secreto y se hizo creer a la opinión pública que el submarino había sido hundido, para que las claves no fuesen cambiadas.

La suma de estos factores obtuvo como resultado el descifrado de los mensajes de Enigma y, por tanto, la drástica disminución de las pérdidas Aliadas en el Atlántico Norte. Ante las sucesivas derrotas, los Alemanes evolucionaron Enigma y crearon una nueva máquina, que más tarde fue vencida.

Bibliografía

[1] *Criptografía y la Máquina Enigma:* http://www.um.es/aulasenior/saavedrafajardo/trabajos/criptografia.pdf

[2] *Simulación de Enigma:* http://enigmaco.de/enigma/enigma_es.html

[3] *Enigma - Wikipedia:* https://es.wikipedia.org/wiki/Enigma_(máquina)

[4] Enigma, el sistema de cifrado que puso en jaque a Europa: https://hipertextual.com/2011/07/la-maquina-enigma-el-sistema-de-cifrado-que-puso-en-jaque-a-europa

[5] *Arthur Scherbius, creador de Enigma:* http://www.abc.es/segunda-guerra-mundial/personajes/20141023/abci-arthur-scherbius-guerra-201410230454.html

[6] *The German cipher machine Enigma:* http://www.matematiksider.dk/enigma_eng.html

[7] *Enigma:* https://www.u-historia.com/uhistoria/tecnico/articulos/enigma/enigma.htm

Bibliografía

[8] *Enigma Cipher Machines:* http://cryptomuseum.com/crypto/enigma/c/index.htm

[9] *La Criptografía en la Hstoria:* https://sites.google.com/site/anilandro4/06112-enigma-01

[10] *Máquinas de cifrado claves para el desenlace de la II Guerra Mundial:* http://www.malavida.com/es/listas/maquinas-de-cifrado-claves-para-el-desenlace-de-la-ii-guerra-mundial-005683#gref

[11] *Códigos secretos en la primera guerra mundial:* https://culturacientifica.com/2015/03/11/codigos-secretos-en-la-primera-guerra-mundial/

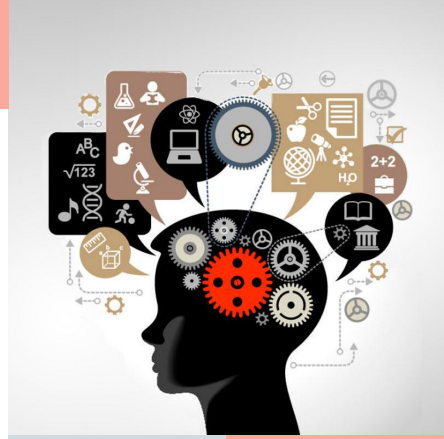
[12] *Criptología Nazi:* http://www2.caminos.upm.es/Departamentos/matematicas/revistapm/revista_impresa/vol_III_num_1/hist_mat_1_crito_nazi.pdf

[13] *La maquina Enigma:* http://www.ejercitos.org/2016/08/28/la-maquina-enigma/

[14] *Posibles Configuraciones de Enigma:* https://crypto.stackexchange.com/questions/33628/how-many-possible-enigma-machine-settings

¡Gracias!

¿Alguna pregunta?



Ana Puertas Olea
Gema Correa Fernández

ETSIIT - Universidad de Granada