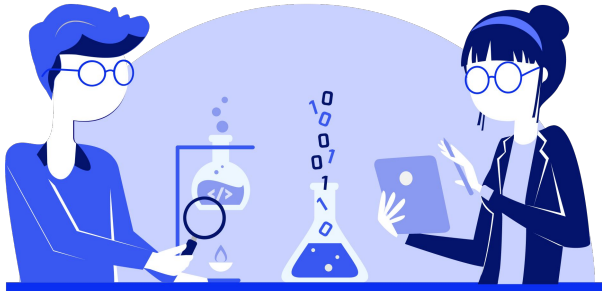
educación IT
CODE YOUR FUTURE

# Criptografía y Blockchain

Módulo 1 - Laboratorio

# Para poder realizar este laboratorio, se recomienda:

- Revisar contenidos previos.



# Ejercicio: Máquina Enigma

En este laboratorio, usaremos una simulación de la máquina Enigma para descifrar mensajes. Existen muchas disponibles en forma online, pero para la práctica usaremos la máquina disponible en [101computing]

1. Imagina que eres operador de la máquina Enigma y que has recibido los siguientes mensajes el 12 de abril de 1940.
    a. OJSBI BUPKA ECMEE ZH
    b. REVNU XWYCV HZFSH NFMSP

> Este emulador es una réplica del proceso de cifrado de la serie Enigma M3, usada por la Marina Alemana (*Kriegsmarine*). El reflector usado es UKW-B. Posteriormente, durante el transcurso de la guerra, fue reemplazada por la serie M4 que incluía un cuarto rotor.

Los **libros de códigos** fueron utilizados por los alemanes para enumerar todas las configuraciones necesarias para las máquinas Enigma, antes de comenzar a cifrar o descifrar mensajes.

Los alemanes solían cambiar la configuración de Enigma muy regularmente (por ejemplo, una vez al día). De este modo, si los aliados lograban romper su código, solo podrían usarlos para ese día y tendrían que encontrar la nueva configuración todos los días.

Los libros de códigos eran documentos altamente confidenciales, ya que si se capturaba o reconstruía un libro de códigos, los mensajes podían descifrarse fácilmente.

Un libro de códigos Enigma tendría una página por mes. La página incluiría todas las configuraciones para cada día del mes con el primer día del mes en la parte inferior de la página, de modo que una vez usada, se podría arrancar una configuración de la página.

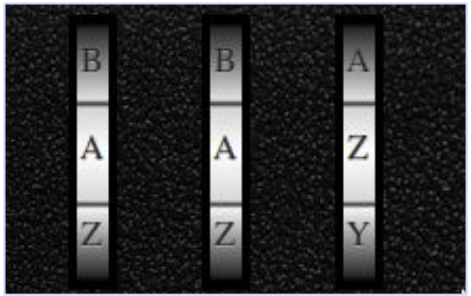
**A continuación, se muestra una sección de un CodeBook para poder realizar el laboratorio**.

2. Si nos fijamos en el día 12, veremos que la configuración de la máquina es la siguiente:
   - Rotores: III I II.
   - *Ring settings* : C K U.
   - *Plugboard settings*: CK IZ QT NP JY GW.
   - Posición inicial de los rotores: VQN.

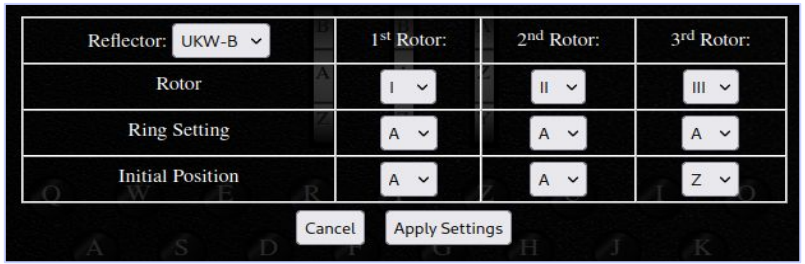
**Enigma M3 Code Book (UKW-B Reflector) - April 1940**

| *Datum* [Date] | *Walzenlage* [Rotors] | *Ringstellung* [Ring settings] | *Steckerverbindungen* [Plugboard settings] | *Grundstellung* [Initial rotor positions] |
|---|---|---|---|---|
| 30 | V III II | AKK | AO HI MU SN VX ZQ | FDV |
| 29 | IV III V | JHS | LW RH UQ VP YM ZA | OTO |
| 28 | IV I II | DIL | EM HL PZ RJ SV UQ | JJK |
| 27 | III I IV | ICC | AX CW FZ KT PO SQ | RXV |
| 26 | IV II III | ECW | GS JD MN OQ VF XH | GUB |
| 25 | V III I | MFO | DW GO HE UF YI ZJ | ZBY |
| 24 | V III I | UCO | GC JU KE MF OD XY | BDT |
| 23 | II V IV | RWQ | BN FK OS PW TA ZE | IYM |
| 22 | IV II I | TRK | BN DU JI OK TF XC | SFX |
| 21 | II V III | CTZ | AF BK GJ VQ XH YT | TQO |
| 20 | I V III | XOM | BX IS LY NF QO WA | DKV |
| 19 | IV V II | LDQ | CR FO LI NM PD XH | IAH |
| 18 | IV I III | NWL | HV IM JB OT QA UF | HSP |
| 17 | II IV III | HFZ | FE IB OQ VC YW ZM | GPZ |
| 16 | II I IV | UBJ | CO GV IH KD ML RB | PJU |
| 15 | I II IV | BCG | ES GD IZ JF LN YA | KFQ |
| 14 | II V IV | EAP | BT CO NE PK VY ZI | CCH |
| 13 | I V II | AOK | CA DZ HK LP RQ YV | DMF |
| 12 | III I II | CKU | CK IZ QT NP JY GW | VQN |
| 11 | II III I | BHN | FR LY OX IT BM GJ | XIO |
| 10 | I V II | QKP | AF HQ IJ OT PB YG | MSW |
| 9 | V I II | UTC | DE FT IP OB UC YL | EQL |

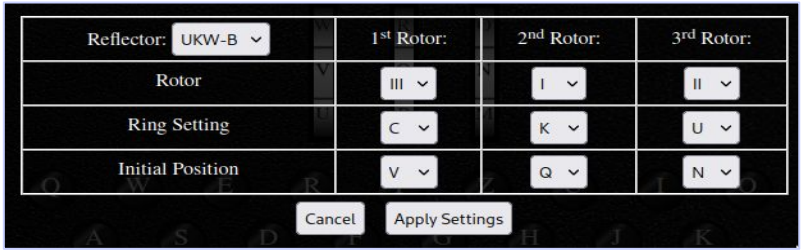
3. En la máquina disponible en el sitio web mencionado, si haces clic sobre los rotores:



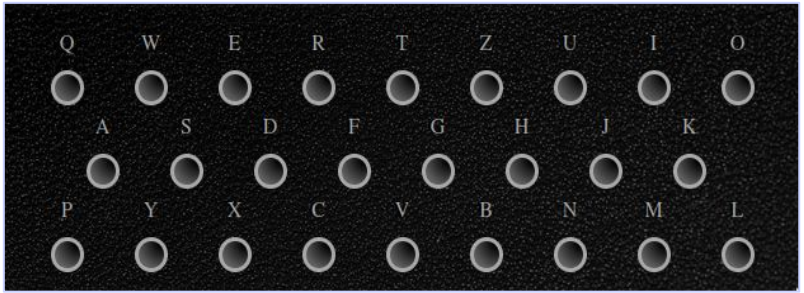

4. Podrás acceder a la configuración:



5. Allí, coloca la configuración del punto anterior:

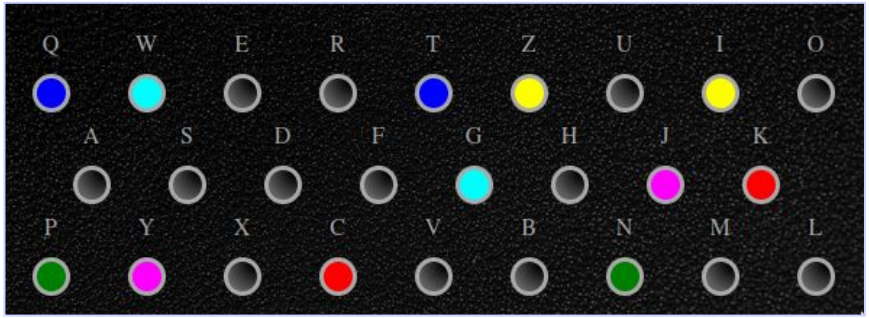



6. Haz clic sobre el botón ***Apply Settings*** para aceptar. En la parte baja de la máquina se encuentra el *plugboard:*



7. Aplica la configuración mencionada más arriba haciendo clic en cada *plug:*

CK IZ QT NP JY GW



Con la máquina configurada, escribe el mensaje y obtendrás el texto descifrado. Antes de descifrar el segundo mensaje, se debe revisar la configuración inicial: todo debería estar igual, excepto la posición inicial de los rotores. Se transcribe el significado de algunas palabras en alemán que pueden formar parte del mensaje.

***Kriegsmarine***: armada Alemana.
***U-Boot: U-Boat.***
***Keine besonderen Ereignisse***: nada para reportar.
***Warten auf Anweisungen***: esperando instrucciones.
***Eins, Zwei, Drei, Vier, Fünf, Sechs, Sieben, Acht, Neun, Zehn***: números del 1 al 10.
***Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Sonntag***: días de la semana (de lunes a domingo).
***Wir sind:*** somos nosotros.
***Wir werden***: vamos a...
***Wir haben***: tenemos.
***Angreifen***: atacar.
***Ziel***: objetivo / ***Ziel zerstört***: objetivo destruido.
***Hafen***: puerto.
***Nächsten***: próximo
***Von: de.***
***Wettervorhersage***: pronóstico climático.

# ¡Sigamos trabajando!