Universidad Nacional Autónoma de México

Facultad de Ingeniería

Práctica 05: Cifrado Enigma

División de Ingeniería Eléctrica

Criptografía

Grupo 02

Semestre 2026-1

Profesor: Dr. Alfonso Francisco De Abiega Pineda

Integrantes:

Camacho Garduño Miguel Angel – 318041188

Chagoya González Leonardo

Gómez Urbano Mariana

Hernández Nava Luisa Fernanda

Rosas Meza Isaías

Vieyra Márquez Andrea

Fecha de entrega: 2 de septiembre de 2025

Práctica 05: Cifrado Enigma

Antecedentes

La máquina de cifrado por rotores fue patentada por el norteamericano Edward H. Hebern en 1917, por el alemán Arthur Scherbius en 1918, por Arvid Gerhard Damm en Suecia y Hugo Alexander Koch en Holanda en 1919.

Debido a las restricciones impuestas a Alemania por el tratado de Versalles, algunas empresas holandesas fabricaban productos de posible uso militar prohibidos a las alemanas. Algunas de estas primeras estaban controladas "a distancia" por Alemania. Flota una teoría de que Koch y su empresa (N. V. Ingenieurbureau Securitas) sólo era una tapadera de los alemanes, quienes controlaban el 60% por medio de Gewerkshaft Securitas, donde trabajaba Scherbius.

En 1923, GS fundó Chiffriermaschinen AG en Alemania, que tras diversos avatares financieros que acabaron en su quiebra, traspasó las patentes a Chiffriermaschinen Gesellshaft Heimsoeth & Rinke, que fabricó las Enigma de la Guerra.

En esencia es un dispositivo electromecánico para cifrar y descifrar mensajes. Estaba orientada a los hombres de negocios para poder transmitir secretos comerciales.

La Wehrmacht se interesó por ella y la transformó para usarla en sus comunicaciones (c. 1935).

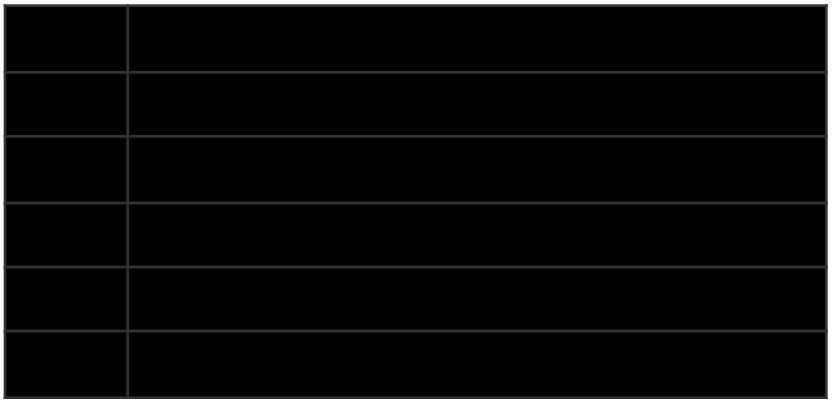
Básicamente consta de un teclado con las veintiséis letras del alfabeto, un reflector, tres rotores (o cuatro en la versión de la Kriegsmarine) y un panel con las correspondientes veintiséis letras con una pequeña bombilla cada una para señalar la correspondencia.

Funcionamiento

Uno de los sistemas más sencillos de encriptar mensajes es la transposición simple, es decir, que cada letra es sustituida por otra. El problema es que por análisis de frecuencia podemos descubrir que si en un mensaje la letra que más se repite es la "l", se puede inferir que está sustituyendo a la "e" la más común en nuestro idioma.

Si, en vez de sustituir la “e” por la “l” siempre, vamos variando la sustitución por diferentes caracteres, el análisis de frecuencias ya no sería tan útil, y con los medios de la época, el trabajo podría ser imposible. Esto es lo que hace básicamente la Enigma.

La Enigma tiene tres rotores (Walzen) con un cableado fijo que establece las transposiciones simples, pero que, al combinarse, pasando la señal por tres, crea una transposición múltiple y variable. Estos rotores se identifican con números romanos. Estas son las correspondencias:

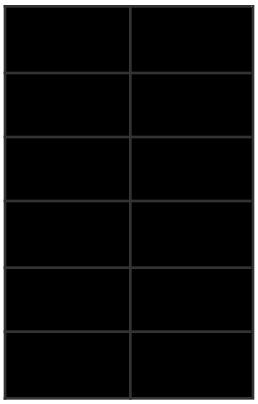


Estos rotores podían intercambiarse de posición, e inicialmente había un juego de cinco, para mayor dificultad.

El reflector (umkehrwalze) es un cableado fijo que hace “reflejarse” la señal de nuevo por los rotores, lo que permite un cifrado y descifrado; es decir, que si con una combinación de tres rotores y en una posición concreta, una A nos queda cifrada como una G, a la inversa, con las mismas condiciones mencionadas, una G nos devolverá una A, lo que permite el descifrado.

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.

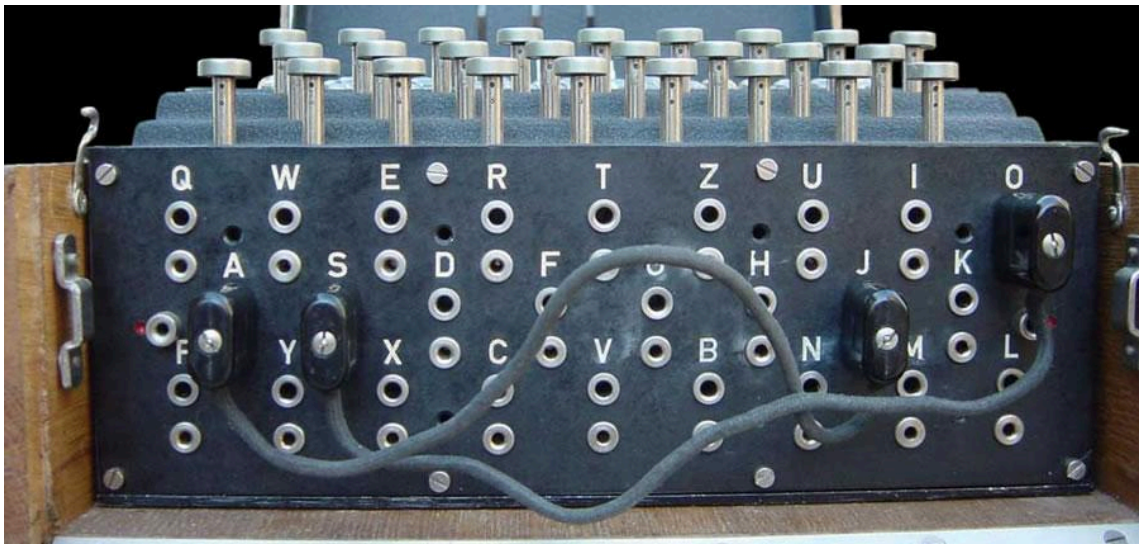
Como si de un cuentakilómetros se tratara, cada pulsación hace avanzar el rotor de la derecha, y al completar una revolución hace avanzar una posición al rotor central, y lo mismo sucede con el izquierdo respecto al central. Los pasos de letras que hacían avanzar al siguiente son:



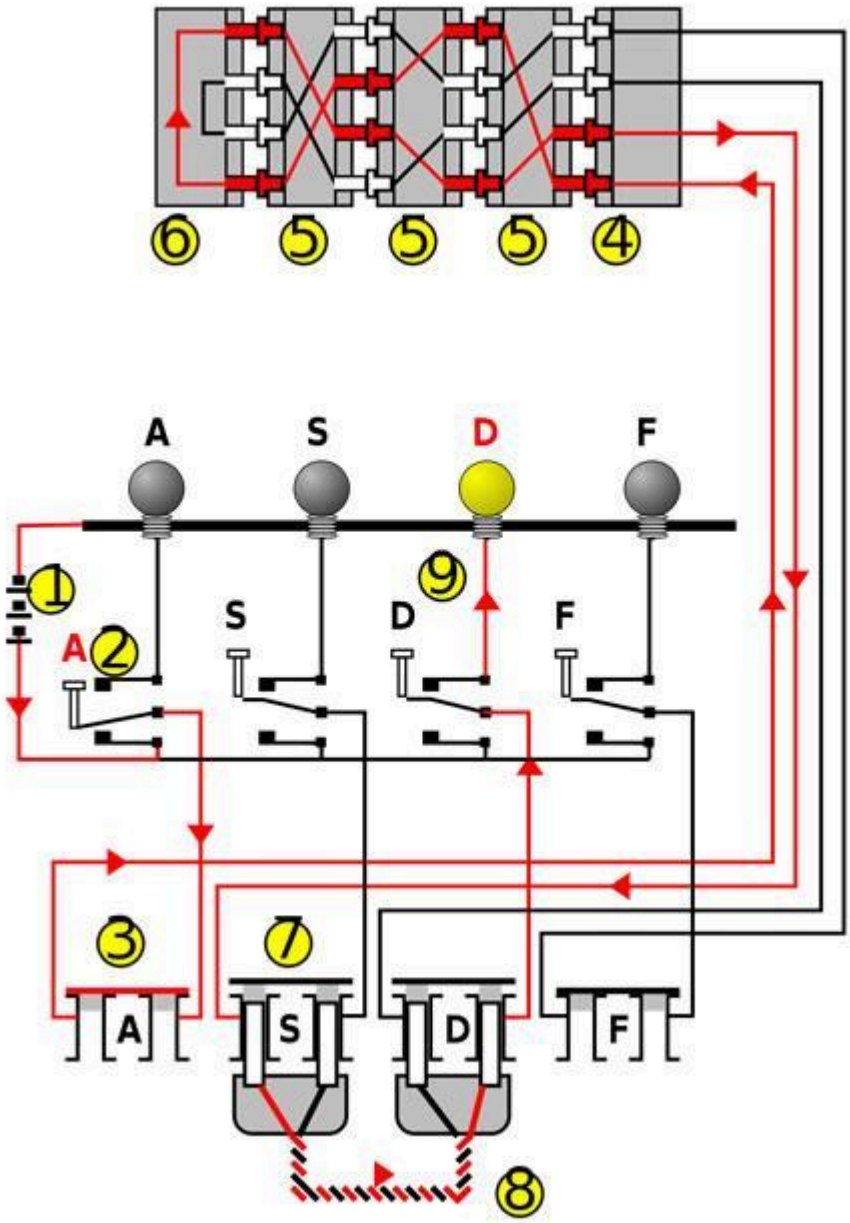
La combinación de los tres rotores da una cifra posible de 17.576 cifras (26 X 26 X 26); es decir, que, si un mensaje tuviera más de 17.576 letras, aparecerían repeticiones.

El panel de clavijas (Steckerbrett) era un conjunto de las veintiséis letras que podían ser puenteadas por medio de unos cables (venían diez con cada máquina) que servían para puentear una letra con otra. Como ejemplo, si conectáramos la F con la R, al teclear una de ellas, sería enviada a los rotores la otra, con lo que aumentaba la complejidad del cifrado.

Con todos estos sistemas, se garantiza que una letra no puede ser cifrada como sí misma.



El proceso de cifrado de una letra



(Suponiendo colocados los rotores I, II y III.)

La señal viaja de derecha a izquierda, y el reflector la devuelve de izquierda a derecha. Su viaje es: teclado, rotor III, II, I, reflector, rotor I, II, III y panel de luces.

Supongamos una Enigma con el reflector B, y los rotores I, II y III, puestos con la clave inicial AAA, y sin puentes en el Steckerbrett.

Tecleamos la letra A.

(Muy importante, al pulsar la letra, el rotor III ha avanzado mecánicamente a B, con lo que en realidad se cifra con la clave AAB, pero se considera la clave anterior, pues es la que se puede visualizar en las ventanas)

Al haber girado el rotor III, con la fuerza de la pulsación, nuestra A entra por la B, que devuelve la D.

Entra en el II, no por D sino por C (recuérdese el desplazamiento), y nos devuelve la D.

En el I la D nos da la F.

En el reflector, la F se refleja de vuelta a los rotores como S.

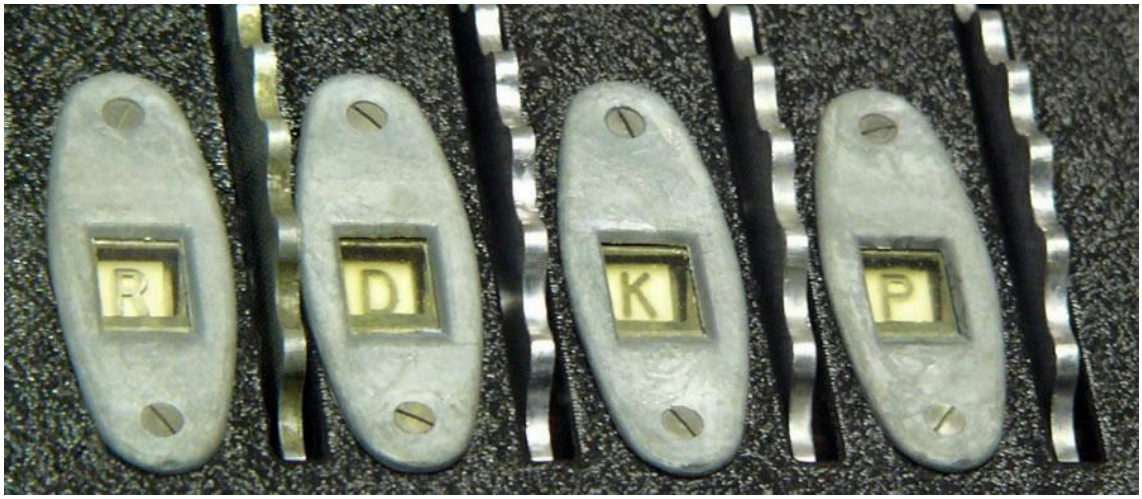
En el I, la S vuelve como S.

En el II, la S pasa a ser una Z.

Y en el III, la Z devolvería la O, pero como ha girado un grado, nos da la B.

La Enigma de la Kriegsmarine

Las comunicaciones fueron especialmente vitales para los U-boote, pues todo el tráfico era vía radio de gran alcance, por lo que el enemigo podía "escucharlas"; por ello la Marina adaptó en 1942 la Enigma con cuatro rotores y diferentes reflectores.



Se añadieron tres rotores:

Y dos extras, el Beta y el Gamma, que se colocaban en la posición más a la izquierda, una cuarta, y que no avanzaban con la revolución completa del tercero, con lo que la cantidad de codificaciones aumentó a 456,976.

La Enigma de la Kriegsmarine o M4, utilizaba unos reflectores diferentes:

Con estas medidas, las Enigma de la Wehrmacht y de la Luftwaffe eran incompatibles con la mucho más compleja y segura de la
Kriegsmarine.

En ambos modelos, los rotores tenían la posibilidad de girar el ánima (con el cableado) respecto a la corona exterior, es decir, que, si giramos estos elementos dos grados, aunque veamos en la ventana la A, internamente estará el cableado de la C; este proceso era llamado Ringstellung, complicando aún más la clave.

El hecho de haber girado el rotor no cambiaba el acarreo, pues dicha muesca era solidaria con la corona exterior.

Según un estudio matemático, la M4, con sus reflectores, los cuatro rotores, su posición variable del ánima y el puenteo de letras, arroja la siguiente cantidad de cifras teóricas:
23.276.989.683.567.292.244.023.724.793.447.227.628.130.289.261.173.376.992.586.381.072.041.865.764.882.821.864.156.921.211.571.619.366.980.734.115.647.633.344.328.661.729.280.000.000.000.000.000.-

Lo que es aproximadamente 2X10E145.

Teniendo en cuenta que la cantidad estimada de partículas subatómicas existentes en el universo es de 2X10E79, la cifra es más que astronómica.

Procedimiento de transmisiones

La transmisión se realiza en Morse, que incluso con malas condiciones de recepción es difícil que se equivoque un operador experimentado.

Como en cualquier comunicación de radio, tras recibir el radiograma, se da el correspondiente acuse de recibo: esto no significa que el mensaje haya sido recibido correctamente. Al ser un mensaje codificado, no hay pauta mental que detecte un posible error, si lo hubiera, sólo se sabrá al descifrar el mensaje, pues al llegar al carácter erróneo, el resto del mensaje será ininteligible, por lo que habrá que pedir una nueva radiodifusión del texto al emisor. El mayor inconveniente es que puede pasar un largo período de tiempo pues quizá el U-boot esté sumergido y no se pueda pedir de nuevo el mensaje hasta mucho después.

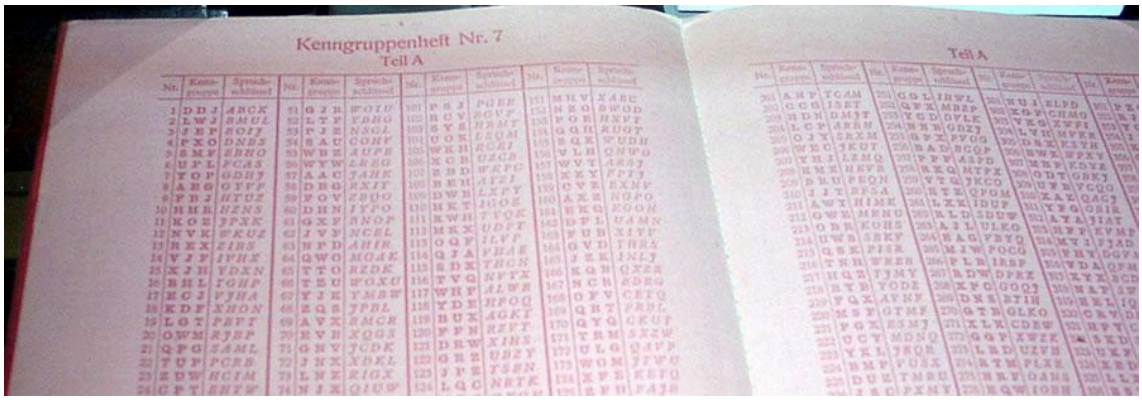
Se establecieron una serie de normas para asegurar al máximo las comunicaciones.

Para cada día, de cada mes, genéricamente, en los libros de claves se especificaba los ajustes de la máquina (estos libros estaban impresos con tinta soluble en agua, para su fácil destrucción):

- Walzenlage: los rotores que debían ser colocados y en qué orden.
- Ringstellung:en que letra se iniciaba cada rotor, el ánima respecto al núcleo.
- Steckerverbindungen: el puenteo de las letras en el steckerbrett.
- Kenngruppen: diversas posibles claves que se camuflaban con otras letras en el encabezamiento del mensaje para codificar.

En la M3, si la clave era RTN, se añadían letras inútiles delante o detrás o en ambas: ERTNP, para descubrir fácilmente la llave (En la M3 se usaban grupos de cinco letras, y la clave constaba de tres, por los rotores.)

En la M4, se agrupaban las letras de a cuatro en el cuerpo de los mensajes, adecuado a los cuatro rotores y a una mayor facilidad mnemotécnica. Al principio y al final del mensaje iba un kenngruppe de tres letras sin codificar que se relacionaba con una clave de cuatro en el Spruchschussel que era la que realmente se usaba para cifrar el cuerpo.



Los libros de claves de la Kriegsmarine constaban de dos partes: la primera o Schlusseltafel M Algemein-Innere Einstellung, indicaba los tres rotores que debían ser usados, su colocación, además del cuarto, el Beta o Gamma, el reflector (B o C). La segunda, Schlusseltafel M Algemein-Aussere Einstellung contenía los conexiones cableadas del Steckerbrett y las posiciones iniciales del día de cada rotor. Esto era conocido como el operativo Triton.

Incluso había una clave extra, llamada Schlussel M NIXE, empleada para la comunicación directa y aún más privada de los oficiales con el BdU, pues otros U-boote no podrían leerla, al ser única para cada nave.

Un mensaje tipo de la Enigma M3 podría ser así:

0900=3TLE=1TL=250=JKF KJN =
KRTNP QJTEE LASBC ...

Mensaje enviado a las nueve horas.
Consta de tres partes.
Primera parte.
Doscientos cincuenta caracteres.
Dos trigramas (clave de sesión)
Cuerpo del mensaje: grupos de cinco letras. El primero lleva camuflado el Kenngruppe (RTN) escogido entre los posibles, que sirve para descifrar la clave de sesión, que la elegía el operador, que está encriptada en los dos trigramas del encabezamiento. Aplicando la

clave del Kenngruppe, nos daría FUH FUH, que es la que usaríamos para descifrar el cuerpo del mensaje, ignorando el primer grupo de cinco letras.
(Esta repetición fue un error que ayudó, entre muchas otras acciones, a romper los códigos por los criptoanalistas de Bletchey Park.)

Para reducir el tamaño de los mensajes, existía el procedimiento llamado Kurzsignalen, que consistía en grupos de cuatro letras que indicaban frases o giros. Como ejemplo podríamos suponer éste: "diríjase de urgencia a toda máquina a la cuadrícula..." podría ser algo así como "PUTP", con lo que al no iniciado en estas Kursignalen un mensaje "au clair" podría parecerle que algo ha fallado al desencriptarlo.

Las Kurzsignalen encontraron su apogeo en 1944. Un proceso del procedimiento Kurzsignaleheft podría ser el que sigue:

Mensaje a enviar:
"GELEITZUG 16-20 DAMPFER
QUADRAT CA 91 33 (se desglosaría como CA 90 y 133)
U-999"
(Traducción: convoy de 16 á 20 vapores en CA 91 33, U-999)
Se usa el Satzbuch para pasarlas a números:
GELEITZUG 16-20 DAMPFER=0512
QUADRAT CA 90=4545
133=8152

Se añade el número que corresponde al día del Schlusselzahlentafel, sin acarreo:

```
 0512  4545  8152
+0384 +0384 +0384
-----  ----  ----
 0890  4829  8436
```

Estas cifras se convierten con el Buchgruppenheft a grupos de cuatro letras:

0890=ZLDP

4829=OYAK

8436=WIKW

Cada U-boot tenía asignada un indicativo, que estaba en el Marinefunknamenliste:

U-999=LQX

El cuerpo del mensaje quedaba así:

ZLDP OYAK WIKW LQX (¡sin cifrar aún por la Enigma!)

Con el Kenngruppeheft del día obteníamos la clave de los cuatro rotores, aunque en el mensaje el Kenngruppe es de tres. Y ahora se cifra el mensaje que quedaría así:

BETA BETA (señal de atención)

RDF (trigrama del kenngruppe, sin cifrar)

QRLE ATMG SIKR (cuerpo del mensaje, cifrado)

ODQ (indicativo del U-boot, cifrado, es parte del cuerpo)

RDF (trigrama repetido, sin cifrar)

El cuerpo del mensaje, para evitar patrones, debía tener un máximo de 250 caracteres. Si se superaba, se enviaban tantas partes como fueran precisas, cada una con su propia clave.

La Enigma solo codificaba las letras del alfabeto, por lo que los números debían se escritos en letras: ein, zwei, drei, vier,... El cero era “nul”, que por razones de seguridad criptográfica, no podía ser repetido; los grupos de dos, tres y cuatro ceros eran sustituidos por “CENTA”, “MILLE” y “MYRIA”.

Para los signos de puntuación, la Kriegsmarine usaba las siguientes combinaciones de letras:

X= punto “.”

Y= coma “,”

UD= interrogación “?”

XX= dos puntos “:”

YY= guión “-”

KK....KK= paréntesis “(....)”

Codificación de un mensaje

En primer lugar, se escribía tipo telegrama.

Después se empleaba el libro de claves Kurzsignalen para acortarlo y complicarlo.

Con la Enigma preparada para el día en cuestión (rotores, reflector, clavijas, puentes y clave) se codificaba.

Transmisión vía radio por Morse.

Ejemplo de mensaje que sería transmitido (con la M4, muy simplificado, anterior a las Kurzsignalen):

U505 VVV BDU 1630 =33=

AMZA AMBB PMDN UPPL PVCK NTWC RZCJ OIIV I

Para el U-505, del BdU(VVV=von, de), enviado a las 16:30, 33 caracteres.

libro de claves para el día:			

Desglose del mensaje	

El mensaje dice: Buena caza camaradas de uhistoria.

Bibliografía

CRIPTOGRAFÍA Y LA MÁQUINA ENIGMA. (s.f.). Recuperado el 28 de agosto de 2025, de https://www.um.es/documents/3239701/10301477/criptografia.pdf/09a15c34-3998-4966-991f-fa9210511080

Macheño Roa, P., & Moreno Basterio, C. (s.f.). *Una Breve Aproximación al Código Nazi: Enigma*. Recuperado el 28 de agosto de 2025, de QED: https://qed.pim.mat.uam.es/revista/articulo/enigma

Manso de Zúñiga Azcue , A. (s.f.). *La Máquina "Enigma"*. Recuperado el 28 de agosto de 2025, de https://www.u-historia.com/uhistoria/tecnico/articulos/enigma/enigma.htm