
**UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO**

**FACULTAD DE INGENIERÍA**


# CRIPTOGRAFÍA

## Reporte: Máquina Enigma

Integrantes:

**Roja Mares Luis Iván**

**Lee Obando Ileana Verónica**

Grupo: **02**

Nombre del Profesor:

**DR. Alfonso Francisco De Abiega L Eglisse**

**Semestre 2026-1**

## 1. Introducción

La Máquina Enigma fue un dispositivo electromecánico diseñado para cifrar y descifrar mensajes de forma automática, desarrollado originalmente en Alemania a inicios del siglo XX.

Aunque en un principio fue concebida para uso comercial, su potencial criptográfico llamó la atención del ejército alemán, que la adoptó como herramienta principal de comunicación segura durante la Segunda Guerra Mundial.

Su fama proviene no solo de la complejidad de su sistema, sino también del papel histórico que desempeñó en el conflicto. El descifrado de los mensajes Enigma por parte de matemáticos polacos y británicos —entre ellos Alan Turing— representó uno de los mayores logros en la historia de la criptografía, sentando las bases de la computación moderna.

---

## 2. Fundamento teórico del Cifrado Enigma

### 2.1. Principio de funcionamiento

La Enigma se basa en el principio de la sustitución polialfabética dinámica, en la que cada letra del mensaje se sustituye por otra, pero la sustitución cambia constantemente gracias a un sistema de rotores. Esto significa que una misma letra puede cifrarse de múltiples maneras, dependiendo de la posición actual de los rotores.

El sistema general está compuesto por los siguientes elementos:

- *Teclado:* Donde el operador introduce las letras del mensaje.

- *Rotores o "Wheels":* Discos giratorios con conexiones internas que realizan sustituciones eléctricas entre las letras. Cada rotor tiene un alfabeto diferente y se mueve automáticamente con cada tecla presionada, modificando el patrón de cifrado.

- *Reflector:* Redirige la señal de retorno a través de los rotores, permitiendo que el proceso de cifrado sea reversible (la misma configuración sirve para descifrar).

- *Panel de Conexiones (Steckerbrett):* Permite intercambiar pares de letras antes y después del paso por los rotores, aumentando exponencialmente el número de combinaciones posibles.

- *Panel de Luces:* Indica la letra cifrada resultante de cada pulsación.

### 2.2. Naturaleza reversible del sistema

Una de las propiedades más notables de Enigma es su simetría, ya que el mismo mecanismo se usa para cifrar y descifrar. Si se introduce el texto cifrado con la misma configuración inicial, la máquina devuelve el texto original.

Esta característica se debe al reflector, que garantiza que el camino eléctrico sea exactamente el mismo en ambos sentidos.

---

## 3. Estructura física y componentes

La Enigma estándar militar (modelo Wehrmacht) tenía la siguiente estructura:

1. **Tres Rotores Principales:** Cada uno con 26 posiciones (una por letra del alfabeto).

2. **Reflector:** Fijo o intercambiable, dependiendo del modelo.

3. **Steckerbrett:** Un panel con 10 pares de enchufes que intercambian letras, como A↔G o M↔P.

4. **Sistema de Engranajes:** Que hace avanzar el primer rotor con cada tecla, y los siguientes de forma análoga al mecanismo de un odómetro.

El número de configuraciones posibles con tres rotores era astronómico:
Más de 150 quintillones ($10^{23}$) de combinaciones distintas, lo que hacía prácticamente imposible un ataque por fuerza bruta con la tecnología de la época.

---

## 4. Proceso de cifrado paso a paso

1. **Configuración Inicial:**
   El operador selecciona la disposición y posición inicial de los rotores (por ejemplo, I-II-III con posiciones A-D-F) y los pares conectados en el tablero.

2. **Entrada de una Letra:**
   Al presionar una tecla, una corriente eléctrica recorre:

   - El Steckerbrett, realizando sustituciones iniciales.
   - Los rotores en secuencia (de derecha a izquierda).
   - El reflector, que redirige la señal de vuelta a través de los rotores.
     El Steckerbrett nuevamente.

     Finalmente, se ilumina una bombilla que indica la letra cifrada.

3. **Rotación de Rotores:**
   Tras cada pulsación, el primer rotor gira una posición; al completar una vuelta completa, hace avanzar el siguiente, generando un nuevo esquema de sustitución con cada letra.

4. **Descifrado:**
   Introduciendo el texto cifrado con la misma configuración inicial, la máquina reproduce el proceso inverso, devolviendo el mensaje original.

## 5. Importancia histórica y criptográfica

El sistema Enigma fue considerado irrompible durante varios años. Sin embargo, matemáticos polacos —Marian Rejewski, Jerzy Różycki y Henryk Zygalski— lograron deducir las configuraciones de la máquina mediante análisis matemático y reconstrucciones mecánicas.
Posteriormente, sus descubrimientos fueron compartidos con los aliados, y en Bletchley Park (Inglaterra), Alan Turing y su equipo desarrollaron la máquina Bombe, diseñada para encontrar la configuración diaria de Enigma de manera automática.

Este avance permitió interceptar y descifrar miles de mensajes alemanes, afectando directamente la estrategia militar nazi y acortando la guerra en varios años, según estimaciones históricas.

---

## 6. Análisis del cifrado

Desde una perspectiva matemática, el cifrado Enigma puede interpretarse como una composición de permutaciones sobre el alfabeto.
Cada rotor implementa una permutación fija, pero su movimiento continuo genera un conjunto de permutaciones que cambian dinámicamente.
El Steckerbrett añade una capa de permutación adicional, y el reflector asegura que el proceso sea involutivo (su propio inverso).

Aunque formidable para su época, el cifrado de Enigma tenía debilidades estructurales:

- Ninguna letra podía cifrarse como sí misma.
- Los mensajes diarios comenzaban con una clave repetida.
- La disciplina operativa alemana (uso repetitivo de frases) facilitó el análisis estadístico.

## 7. Simulación moderna

Actualmente, existen simuladores digitales de la Máquina Enigma que reproducen con precisión su comportamiento mecánico.
Estos programas permiten experimentar con diferentes configuraciones de rotores, paneles de enchufes y reflectores, mostrando en tiempo real el proceso de cifrado y descifrado.

En el contexto de la materia de Criptografía, estudiar la Enigma permite comprender:

- La transición entre la criptografía clásica y los sistemas electromecánicos.
- Cómo la seguridad depende tanto del algoritmo como del manejo de las claves.
- La evolución hacia la criptografía computacional moderna.

---

## 8. Conclusiones

La Máquina Enigma representa un punto de inflexión en la historia de la criptografía.
Su diseño combina principios matemáticos, ingeniería eléctrica y mecánica de precisión, anticipando los conceptos de la seguridad digital moderna.

Aunque finalmente fue vulnerada, su complejidad impulsó el desarrollo de las primeras máquinas automáticas de cálculo, como la Bombe y el Colossus, consideradas antecesoras directas de los computadores actuales.

En el ámbito académico, el estudio de Enigma es esencial para comprender:

- Los límites de la criptografía manual y mecánica.
- La importancia de la gestión de claves y protocolos de seguridad.
- La evolución de la criptografía hacia los algoritmos de clave pública y simétrica actuales.

En suma, Enigma no solo fue una herramienta de guerra, sino el origen práctico de la criptografía moderna.

## Referencias Bibliográficas


1. Soler Fuensanta, J. R. (n. d.). *Enigma en España. Un resumen de su historia desde su aparición hasta su retiro final* [PDF]. Criptohistoria. Recuperado de https://www.criptohistoria.es/files/enigma_espana.pd

2. Ministerio de Defensa. (2020, julio 8). *Máquina Enigma – K-296. El modelo K de la singular máquina de cifrado alemana* [PDF]. Recuperado de https://www.defensa.gob.es/Galerias/gabinete/red/2020/07/p-56-61-red-374-criptografia.pdf

3. Fundación Telefónica. (2018, abril 23). *Máquina enigma: Comunicación codificada*. Recuperado de https://www.fundaciontelefonica.com/exposiciones/maquina-enigma-comunicacion-codificada/

4. Universidad de Murcia. (n. d.). *Criptografía y la máquina Enigma* [PDF]. Recuperado de https://www.um.es/documents/3239701/10301477/criptografia.pdf/09a15c34-3998-4966-991f-fa9210511080

5. Xifré Solana, P. (2009). *Antecedentes y perspectivas de estudio en historia de la Criptografía* [PDF]. e-Archivo UC3M. Recuperado de https://e-archivo.uc3m.es/bitstreams/0deac081-c318-47b7-9fba-f0b4e39da4bc/download