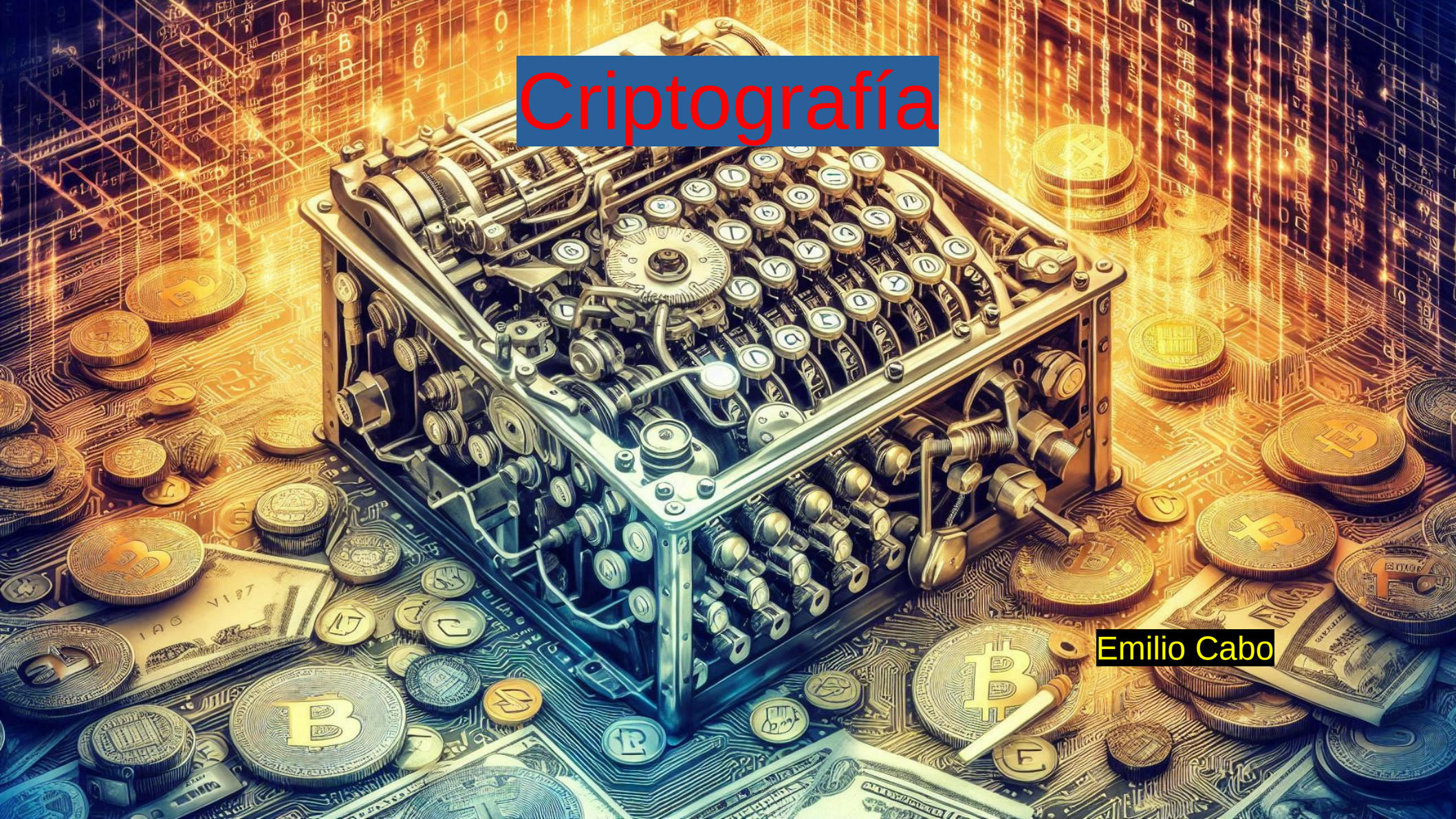
Criptografía



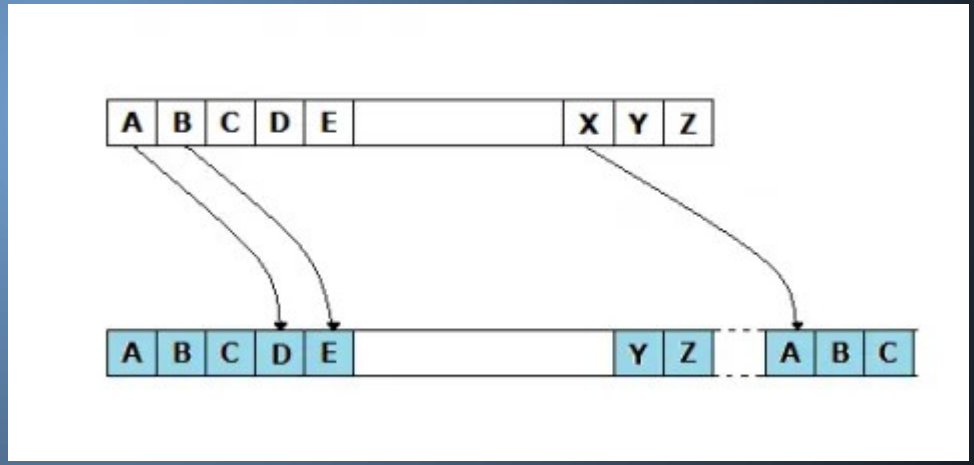
Emilio Cabo

Primer criptograma

- Primer uso de la criptografía que se encontró en una inscripción tallada alrededor de 1900 a. C., en la cámara principal de la tumba del noble Khnumhotep II

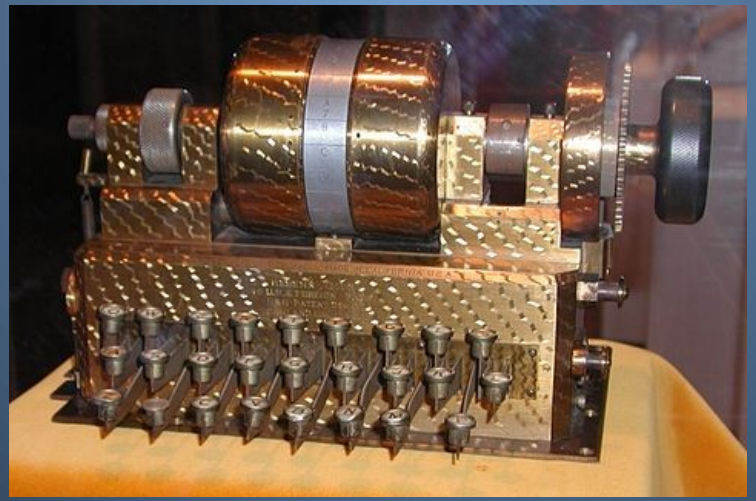
Julio César

- Año 100 a.C.: Julio César utiliza un cifrado para mensajes secretos.
- Importancia: Primer cifrado histórico mencionado en la literatura académica.
- Funcionamiento: Cada carácter se desplaza 3 lugares.



Máquina rotor de Hebern

- Con la proliferación de las máquinas electro-mecánicas. Año 1918
- Introducido el mensaje desde partes de una máquina de escribir mecánica estándar.
- Se cifraba el mensaje mediante un cilindro codificador.



Funcionamiento de la encriptación

- El operario gira el rotor para que tenga una posición inicial.
- Cada pulsación: El rotor giraba, cambiando ligeramente el alfabeto de sustitución.
- Una máquina con 1 rotor que tenga 26 letras da 26^1 posibilidades
- Máquina con 5 es 26^5 posibilidades = 11,881,376

Máquina Enigma

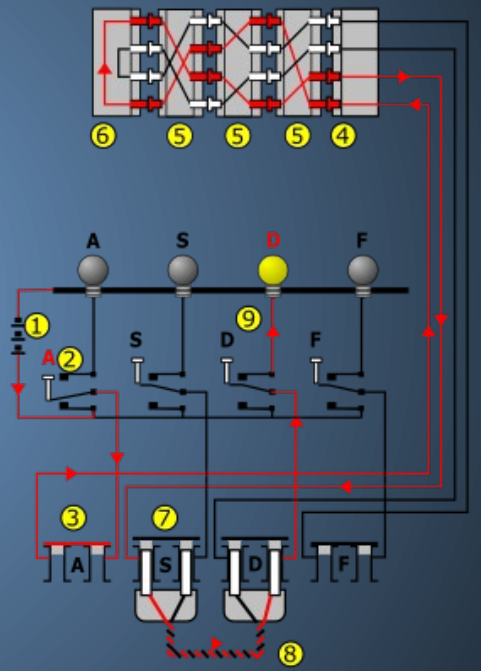
- Diseñada para la encriptación de comunicaciones alemanas.
- Disponía de 5 rotores cómo la máquina de Hebern.
- Giraban a distinta velocidad.

Funcionamiento Enigma

- Consta de un teclado y un sistema de luces.
- El operador escribe el mensaje en el teclado
- Las luces encima muestran el texto cifrado.
- Sistema de enchufes. Cada letra se asignaba a otra. Esto permitía cada día cambiar la encriptación.
- Esto se sumaba a la encriptación de los rotores

Conjunto de posibilidades

- Elige 3 rotores de un conjunto de 5 rotores = 5 x 4 x 3 = 60
- 26 posiciones por rotor = 26 x 26 x 26 = 17,576
- Tablero de conexiones = 26! / (6! x 10! x 2^10) = 150,738,274,937,250
- Multiplica cada uno de los anteriores = 158,962,555,217,826,360,000



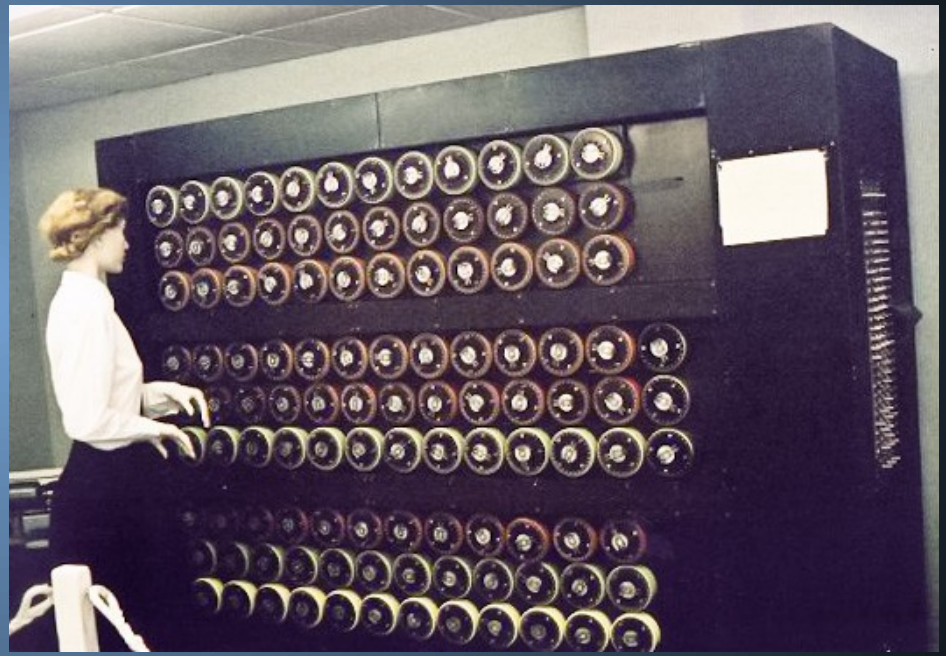
Simulador Enigma

Bletchey park

- Ubicación: Centro de descifrado de códigos del Reino Unido durante la Segunda Guerra Mundial.
- Propósito: Romper los códigos de comunicación del enemigo, especialmente los cifrados por la máquina Enigma

Le Bombe

- Diseño y Desarrollo: Creado en 1939 por Alan Turing y refinado por Gordon Welchman, con ingeniería de Harold Keen2.
- Funcionamiento: simulaba varias máquinas Enigma para descifrar mensajes cifrados durante la Segunda Guerra Mundial. Utilizaba un proceso de eliminación para descartar configuraciones incorrectas, descubriendo los ajustes diarios de las máquinas Enigma.



Bitcoin y Satoshi Nakamoto

- Creación de Bitcoin: Publicó el documento técnico de Bitcoin en 2008 y lanzó la red en 2009.
- Permite transferencias sin una autoridad central que certifique los saldos

Identidad secreta

- Minería Inicial: Nakamoto minó aproximadamente 1.1 millones de Bitcoins
- Fortuna 70 mil millones de dólares
- ataques del 51%