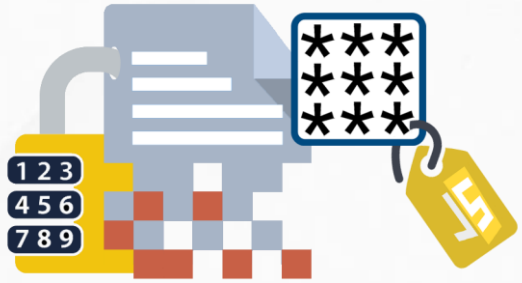
UNEMI
UNIVERSIDAD ESTATAL DE MILAGRO

Sistemas Operativos

TECNOLOGÍAS DE LA INFORMACIÓN EN MODALIDAD EN LÍNEA

CRIPTOGRAFIA



GRUPO B

Contenidos

1: Definiciones
2: Inicios
3: Maquinas Electromecánicas
4: Era Digital
5: El Futuro
6: Demostración Practica

Definiciones

La criptografía es la técnica utilizada para cifrar mensajes que contienen información, palabra que proviene del griego **Kryptos** y **Graphein**, que significan "**escondido**" y "**escritura**", respectivamente;

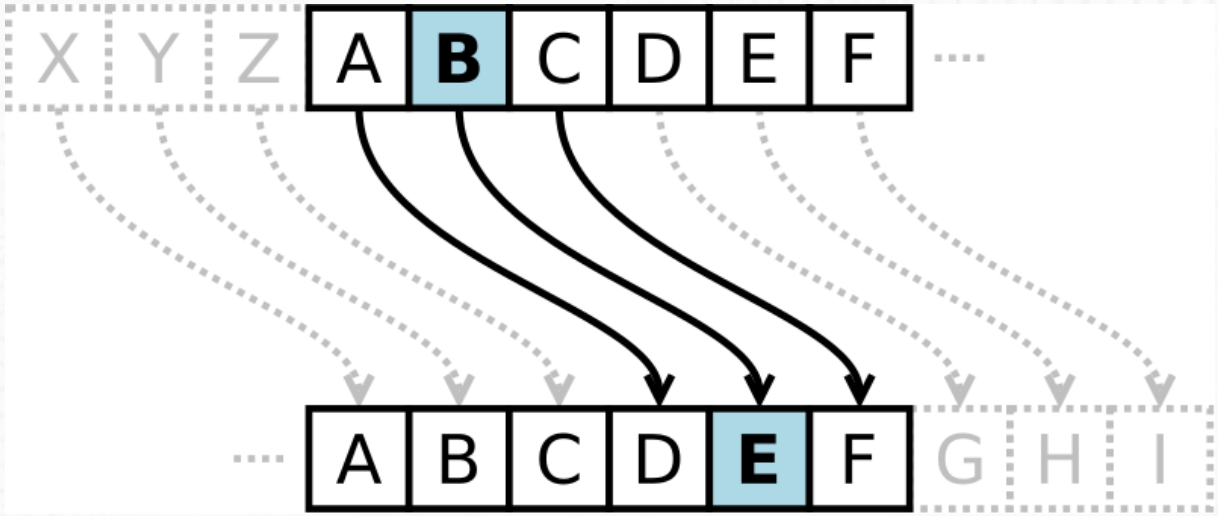
La criptografía es parte de la criptología (del griego **Kriptos** = **oculto** y **Logos** = **ciencia** o estudio);

Criptoanálisis, tiene como objeto el descifrado de la información procesada por algún criptosistema, es decir, que se encuentre cifrada. **(Pabón Cadavid, 2024)**

Ilustración futurista sobre criptografía, representando elementos de seguridad digital, claves criptográficas y flujos de datos encriptados. Generado por inteligencia artificial con DALL·E, bajo solicitud de Claudio Borja.

Inicios

La **criptografía** ha evolucionado desde sus inicios hasta convertirse en una disciplina esencial en la seguridad de la información. Los cifrados clásicos, se basaban en técnicas de sustitución y transposición para ocultar el contenido de los mensajes, un ejemplo emblemático es el cifrado **César**, utilizado por **Julio César**, que consistía en desplazar las letras del alfabeto un número fijo de posiciones, aunque son vulnerables a análisis de frecuencia y otros métodos de criptoanálisis rudimentarios. **(Arenas Vega, 2004)**

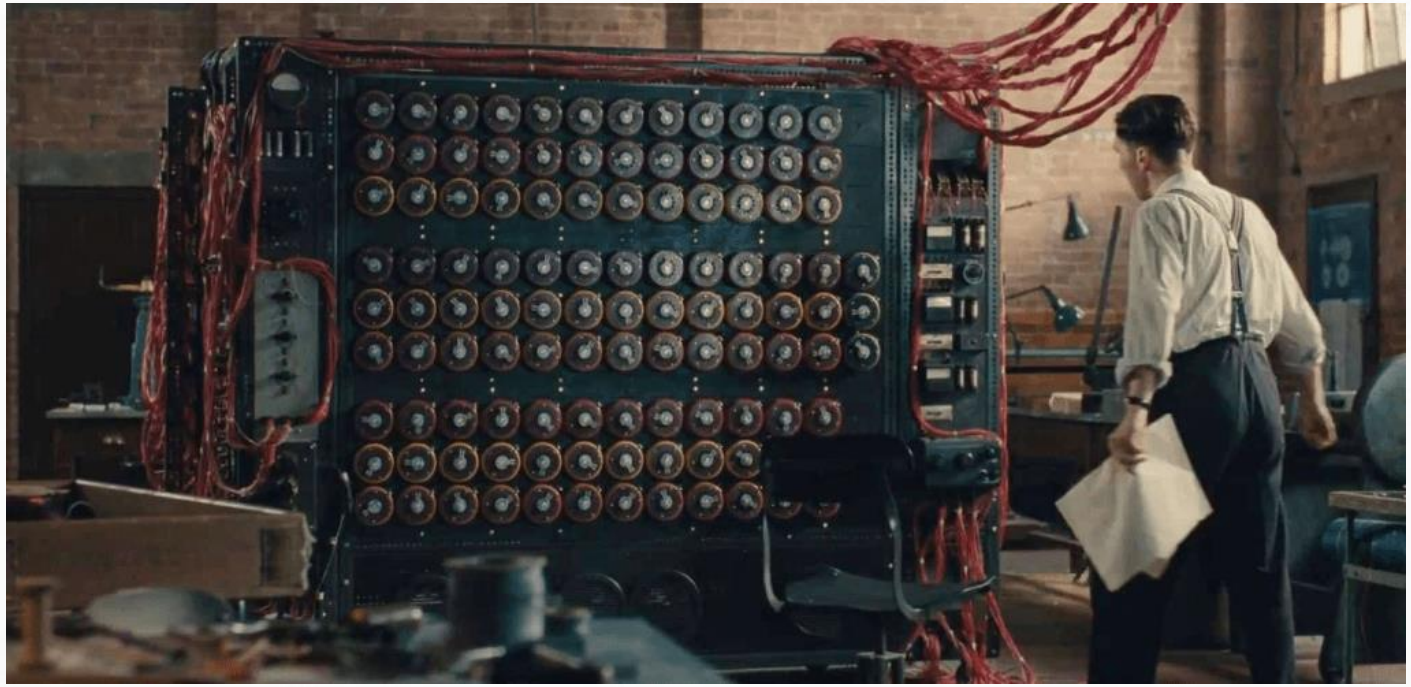


El cifrado César mueve cada letra un determinado número de espacios en el alfabeto. En este ejemplo se usa un desplazamiento de tres espacios, así que una B en el texto original se convierte en una E en el texto codificado

Máquinas Electromecánicas

El siglo XX marcó un punto de inflexión con la introducción de máquinas electromecánicas para el cifrado, como la máquina Enigma utilizada por Alemania durante la Segunda Guerra Mundial, el trabajo de Alan Turing y otros criptógrafos en Bletchley Park para descifrar Enigma no solo fue crucial para el desenlace de la guerra, sino que también sentó las bases para la criptografía moderna y la computación. **(Arenas Vega, 2004)**

Máquina Enigma en el Museo Nacional de la Ciencia y la Tecnología Leonardo da Vinci, Milán

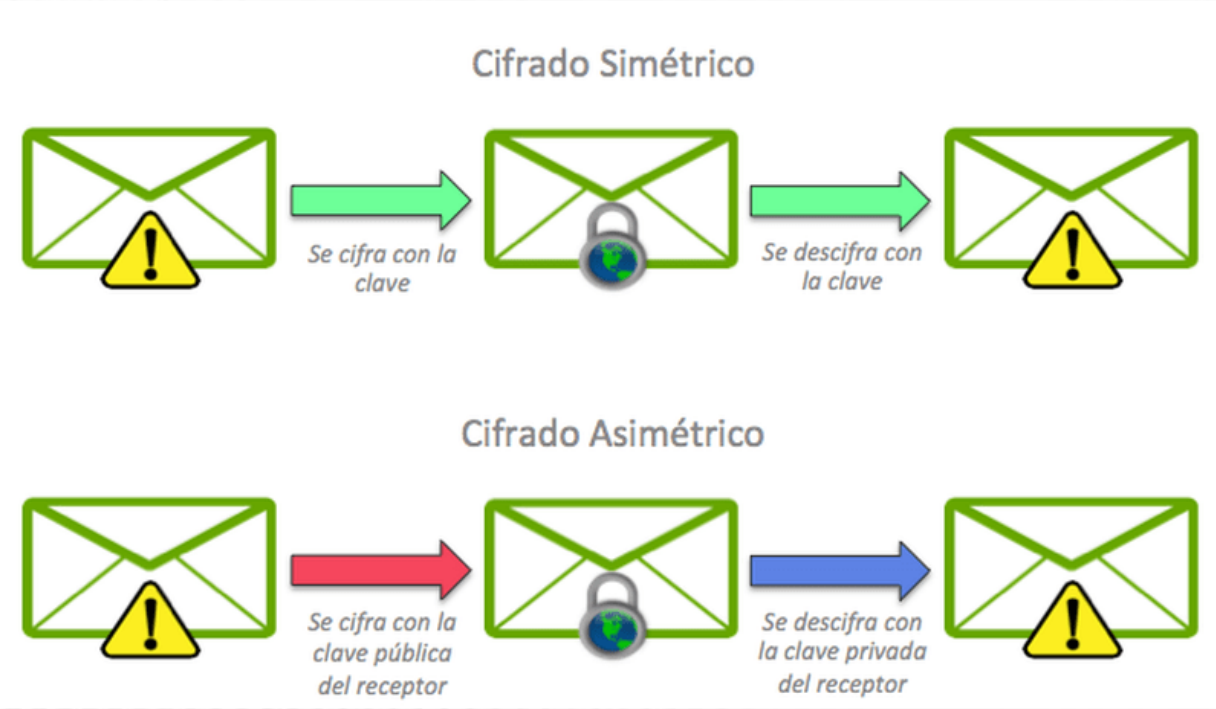


Escena de la película: El Código Enigma – Alan Turing

Era Digital

La criptografía ha incorporado complejos algoritmos matemáticos y teorías avanzadas, se han desarrollado sistemas de cifrado simétrico, como el Estándar de Cifrado Avanzado (AES), y asimétrico, como RSA, que permiten comunicaciones seguras en redes abiertas como Internet, la criptografía de clave pública ha facilitado la implementación de firmas digitales y protocolos de seguridad esenciales para el comercio electrónico y otras aplicaciones.

(Arenas Vega, 2004)



"Ilustración comparativa de los métodos de cifrado: simétrico, donde se utiliza la misma clave para cifrar y descifrar, y asimétrico, que emplea una clave pública para cifrar y una clave privada para descifrar."

Futuro

La criptografía cuántica se basa en los principios de la mecánica cuántica para garantizar la seguridad de la información, a diferencia de la criptografía tradicional que depende de la complejidad matemática de ciertos problemas. Esta diferencia fundamental implica que, mientras la criptografía clásica puede ser vulnerable a ataques con suficiente poder computacional, la cuántica ofrece una seguridad basada en las leyes físicas, lo que la hace teóricamente invulnerable a tales ataques.

(IBM, 2025)

La llegada de la computación cuántica plantea amenazas significativas para los algoritmos criptográficos actuales, ya que estos nuevos ordenadores podrían resolver problemas matemáticos complejos en tiempos mucho más cortos, comprometiendo la seguridad de los sistemas tradicionales.

Para mitigar estos riesgos, se están desarrollando propuestas de cifrado post-cuántico, que buscan crear algoritmos resistentes a los ataques de la computación cuántica, asegurando así la protección de la información en el futuro.

(Fundacionbankinter, 2025)

Demostración Practica 1

UNEMI
UNIVERSIDAD ESTATAL DE MILAGRO

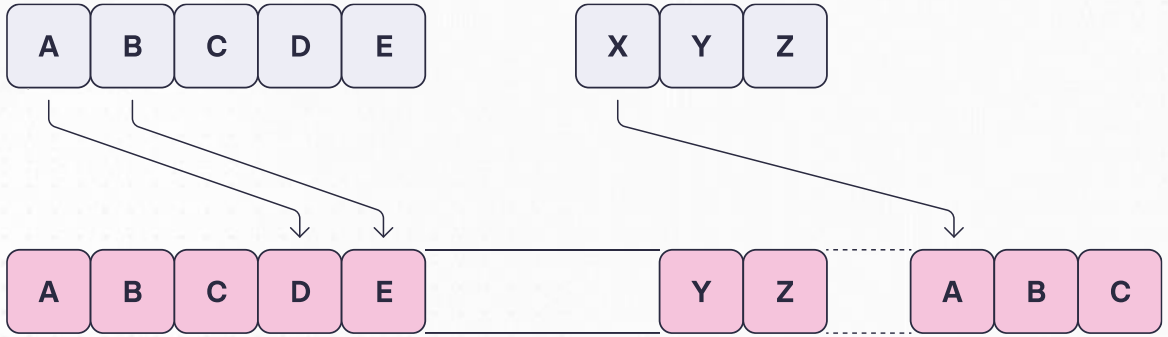
A	B	C	D	E	F	G	H	I	J	K	L	M
Z	Y	X	W	V	U	T	S	R	Q	P	O	N

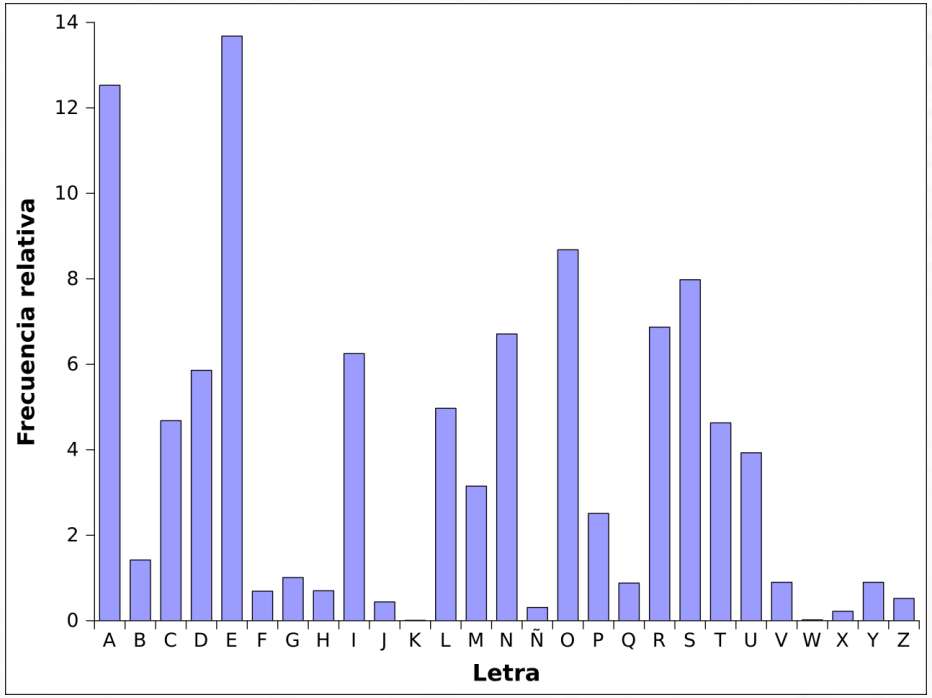
Cifrado Atbash

Sustitución Simple

Demostración Practica 2

UNEMI
UNIVERSIDAD ESTATAL DE MILAGRO





Cifrado Cesar

Sustitución Simple

Demostración Practica 3
Cifrado HILL SUSTITUCIÓN POLIGRÁFICA

UNEMI
UNIVERSIDAD ESTATAL DE MILAGRO

RECUADRO MÉTODO DE HILL																								
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	Z	Y	Z	_
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Paso 1 - Convertir el texto a números: Asignamos valores a las letras según su posición en el alfabeto.
Omitimos los espacios y usamos pares de letras.
Texto: **SISTEMAS OPERATIVOS GRUPO B UNEMI**

Letra	S	I	S	T	E	M	A	S		O	P	E	R	A	T	I	V	O	S		G	R	U	P	O		B		U	N	E	M	I
Valor	18	8	18	19	4	12	0	18	26	14	15	4	17	0	19	8	21	14	18	26	6	17	20	15	14	26	1	26	20	13	4	12	8

Necesitamos un número **par de caracteres** (porque estamos usando una matriz 2×2).
El texto original tiene 33 caracteres, por lo que agregamos una **"X" (23)** como relleno al final para completar el par.

Texto numérico con relleno:
(18,8),(18,19),(4,12),(0,18),(26,14),(15,4),(17,0),(19,8),(21,14),(18,26),(6,17),(20,15),(14,26),(1,26),(20,13),(4,12),(8,23)(18,8),……, (8,23)

Demostración Practica 3

UNEMI
UNIVERSIDAD ESTATAL DE MILAGRO

$$A) = \begin{bmatrix} 18 & 8 \\ 18 & 19 \\ 4 & 12 \\ 0 & 18 \\ 26 & 14 \\ 15 & 4 \\ 17 & 0 \\ 19 & 8 \\ 21 & 14 \\ 18 & 26 \\ 6 & 17 \\ 20 & 15 \\ 14 & 26 \\ 1 & 26 \\ 20 & 13 \\ 4 & 12 \\ 8 & 23 \end{bmatrix}$$

Paso 2: Selección de la Matriz Clave

Usamos la matriz **K**: $\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$

Este es un punto clave, ya que la matriz debe ser invertible en **módulo 27** para que el texto cifrado pueda descifrarse correctamente.

Paso 3: Multiplicación de Matrices

Para cifrar, usamos la ecuación: $C = KxP \ mod\ 27$

Donde:

- **P** es un vector con los valores de cada par de letras.
- **K** es la matriz clave.
- **C** es el resultado cifrado.

Ejemplo con el primer par **(18,8):**

$$C = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix} \text{x} \begin{bmatrix} 18 \\ 8 \end{bmatrix} mod\ 27$$

$$C = \begin{bmatrix} 3x18 + & 3x8 \\ 2x18 + & 58 \end{bmatrix} mod\ 27$$

$$C = \begin{bmatrix} 78\ mod\ 27 \\ 76\ mod\ 27 \end{bmatrix}$$

$$C = \begin{bmatrix} 24 \\ 22 \end{bmatrix}$$

Convertimos estos valores a letras:

24 → Y
22 → W

El primer par (18,8) se cifró como "YW".

Hacemos lo mismo con todos los pares y obtenemos el texto cifrado completo:

Texto: **SISTEMAS OPERATIVOS GRUPO B UNEMI**

Texto Cifrado: **YWDXVOAJMODXYHAYYEYEPQYHMXAYSYVOMX**

BIBLIOGRAFÍA

Pabón Cadavid, J. (2024). The cryptography and the protection of digital information. La Propiedad Inmaterial.

¿Qué es la criptografía cuántica? (2024, mayo 6). Ibm.com. https://www.ibm.com/es-es/topics/quantum-cryptography?

Edu.co. Recuperado el 7 de febrero de 2025, de https://revistas.uexternado.edu.co/index.php/propin/article/view/2476/3636