Guía del Asistente

Curso: Introducción a la Criptografía con Aplicaciones Prácticas

Luis Alejandro Pérez Sarmiento

22 de julio de 2025

1. Objetivo del Curso

Este curso tiene como objetivo introducir los principios fundamentales de la criptografía moderna, a partir de ejemplos históricos simples hasta aplicaciones reales como el cifrado de imágenes con AES.

2. Conceptos Clave

- Confidencialidad: Solo el destinatario debe poder leer el mensaje.
- Integridad: El mensaje no ha sido modificado.
- Autenticidad: El origen del mensaje es legítimo.

Preguntas para reflexionar

- ¿Cuál crees que es el concepto más importante en un mensaje bancario?
- ¿Puedes pensar en una situación donde la integridad sea más crítica que la confidencialidad?

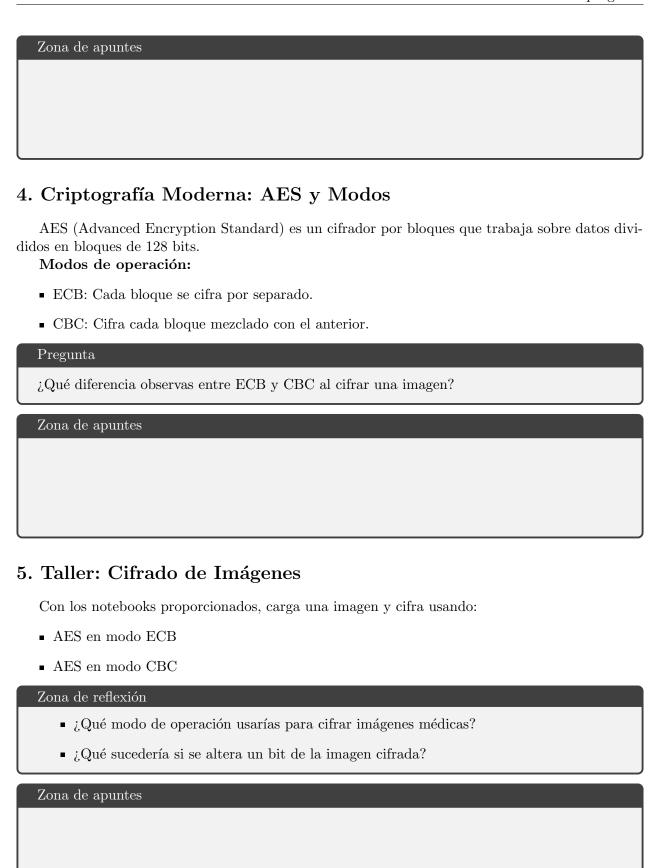
3. Cifrado por Sustitución: César

El cifrado César consiste en reemplazar cada letra por otra que se encuentre un número fijo de posiciones más adelante en el alfabeto.

Ejemplo: Con desplazamiento 3, la A se convierte en D, la B en E, etc.

Actividad práctica

Cifra el mensaje "HOLA MUNDO" con un desplazamiento de 5.



6. Autoevaluación Final

- 1. ¿Cuál es la diferencia entre confidencialidad e integridad?
- 2. ¿Por qué el modo ECB puede filtrar información visual?
- 3. ¿Qué ventajas ofrece CBC frente a ECB?

7. Recursos Recomendados

- Khan Academy: https://es.khanacademy.org/computing/computer-science/cryptography
- Libro: Ïntroduction to mathematical cryptography"de Jeffrey Hoffstein
- Python Cryptodome: https://pycryptodome.readthedocs.io