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.

Zona de apuntes

4. Criptografía Moderna: AES y Modos

AES (Advanced Encryption Standard) es un cifrador por bloques que trabaja sobre datos divididos en bloques de 128 bits.

Modos de operación:

- ECB: Cada bloque se cifra por separado.
- CBC: Cifra cada bloque mezclado con el anterior.

Pregunta

¿Qué diferencia observas entre ECB y CBC al cifrar una imagen?

Zona de apuntes

5. Taller: Cifrado de Imágenes

Con los notebooks proporcionados, carga una imagen y cifra usando:

- AES en modo ECB
- AES en modo CBC

Zona de reflexión

- ¿Qué modo de operación usarías para cifrar imágenes médicas?
- ¿Qué sucedería si se altera un bit de la imagen cifrada?

Zona de apuntes

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