

# SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

[Área personal](#) / [Mis cursos](#) / [SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN](#) / [Unidad # 3 Descripción: Análisis de los ataques d...](#)  
/ [Taller No. 4 \( 2do. Parcial \)](#)

## Taller No. 4 ( 2do. Parcial )

**Apertura:** Thursday, 27 de July de 2023, 20:00

✓ Hecho

Observar el siguiente video y en la plataforma de forma directa indicar para usted cuál o cuales ( máximo 2 ) es o son el algoritmos o los algoritmos que deberían ser usados y por qué. Recordar que su respuesta no debe exceder las 200 palabras. Esta actividad estará disponible hasta las 22h00 del 27 de Julio.



### Estado de la entrega

Estado de la entrega	Enviado para calificar
Estado de la calificación	Calificado
Última modificación	Thursday, 27 de July de 2023, 20:45


#### Texto en línea

- Los algoritmos que yo recomendaría son:
- Algoritmo de clave secreta:** AES (Advanced Encryption Standard) El AES es un algoritmo de cifrado de clave secreta ampliamente utilizado y considerado seguro. Fue seleccionado por el Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos para reemplazar al DES debido a su mayor seguridad. AES opera en bloques de 128 bits y admite claves de 128, 192 y 256 bits, lo que lo hace adecuado para una amplia gama de aplicaciones.
  - Modalidad de cifrado:** CBC (Cipher Block Chaining) CBC es una modalidad de cifrado que mejora la seguridad del cifrado por bloques al agregar la retroalimentación del bloque cifrado anterior al siguiente bloque antes de cifrarlo. Cada bloque depende del bloque anterior, lo que aumenta la resistencia a ataques conocidos como "ataques de texto plano seleccionado" y mejora la seguridad general. Sin embargo, CBC no es adecuado para paralelización debido a su naturaleza secuencial.

Comentarios de la entrega

Comentarios (0)

Comentario

Calificación	10,00 / 10,00
Calificado sobre	Tuesday, 22 de August de 2023, 17:25
Calificado por	<div> OTTO RODRIGO GONZALEZ MENDOZA</div>

[← Tarea No. 3 \( 2do. Parcial \)](#)

Ir a...

[Material Usado en Clases ▶](#)

Usted se ha identificado como BETZABETH MADELINE MUÑOZ VILLEGAS (Cerrar sesión)

Reiniciar tour para usuario en esta página

15150059\_15150091\_1515816

[Español - Internacional \(es\)](#)

[English \(en\)](#)

[Español - Internacional \(es\)](#)

[Resumen de retención de datos](#)

[Descargar la app para dispositivos móviles](#)