

# 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. 3 \( 2do. Parcial \)](#)

## Taller No. 3 ( 2do. Parcial )

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

✓ Hecho

En el siguiente enlace: [https://ugye-my.sharepoint.com/:b/g/personal/otto\\_gonzalezm\\_ug\\_edu\\_ec/ESfBpL5NMI1AqLOdSmc0I9gBdbtsoVfedj5zeREIE30XqA?e=mRcuKc;](https://ugye-my.sharepoint.com/:b/g/personal/otto_gonzalezm_ug_edu_ec/ESfBpL5NMI1AqLOdSmc0I9gBdbtsoVfedj5zeREIE30XqA?e=mRcuKc;)

Descargar el documento, leerlo y en la plataforma de forma directa responder a las siguientes preguntas:

- ¿Cuál es la o las diferencia (s) de la criptografía simétrica y la criptografía asimétrica?
- ¿Para qué son útiles las funciones HASH?
- ¿Qué es la criptografía Híbrida? y ¿Cuál sería su aplicabilidad?

Esta actividad estará disponible hasta las 22h00 del Jueves 20 de Julio .

## Estado de la entrega

Estado de la entrega	Enviado para calificar
Estado de la calificación	Calificado
Última modificación	Thursday, 20 de July de 2023, 21:29

Texto en línea



¿Cuál es la o las diferencia (s) de la criptografía simétrica y la criptografía asimétrica?

La criptografía simétrica utiliza una única clave secreta para cifrar y descifrar la información. Tanto el emisor como el receptor deben conocer y compartir esta clave antes de la comunicación. Es más rápida y eficiente para cifrar grandes volúmenes de datos, pero presenta el desafío de cómo compartir de manera segura la clave entre las partes.

En cambio, la criptografía asimétrica utiliza un par de claves matemáticamente relacionadas: una clave pública y una clave privada. El emisor utiliza la clave pública del receptor para cifrar el mensaje, y solo el receptor, que posee la clave privada correspondiente, puede descifrarlo. Esto elimina la necesidad de compartir una clave secreta, pero el proceso de cifrado y descifrado es más lento y requiere más recursos.

¿Para qué son útiles las funciones HASH?

Las funciones HASH son útiles para crear resúmenes o huellas digitales únicas y fijas de datos de cualquier tamaño. Estas funciones toman un conjunto de datos como entrada y generan una cadena de longitud fija, que actúa como una especie de "huella digital" de los datos originales.

¿Qué es la criptografía Híbrida? y ¿Cuál sería su aplicabilidad?


La criptografía híbrida combina la criptografía simétrica y asimétrica para obtener los beneficios de ambas. En este enfoque, se utiliza la criptografía asimétrica para establecer una conexión segura y compartir una clave simétrica única y temporalmente para la comunicación.

Su aplicabilidad es muy común en la seguridad de la comunicación en línea, como en aplicaciones de mensajería y transacciones en línea. Al utilizar la criptografía asimétrica para intercambiar claves simétricas y luego la criptografía simétrica para cifrar los datos reales, se logra un equilibrio entre seguridad y eficiencia.

Comentarios de la entrega

▶ [Comentarios \(0\)](#)

Comentario

Calificación	10,00 / 10,00
Calificado sobre	Sunday, 23 de July de 2023, 22:10
Calificado por	<div> OTTO RODRIGO GONZALEZ MENDOZA</div>

◀ [Material Usado en Clases](#)

Ir a...

Tarea No. 3 ( 2do. Parcial ) ▶

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