COLOMBIA POTENCIA DE LA VIDA

TIC

CRIPTOGRAFÍA

Lección 2

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

Universidad Tecnológica de Pereira

Tiempo de ejecución: 6 horas

PLANTEAMIENTO DE LA SESIÓN
En la segunda sesión se los algoritmos de cifrados modernos hechos con sistemas computacionales, teniendo conocimientos de los sistemas antiguos y sus limitaciones, ahora los estudiantes adquieren el contexto del mundo actual y el avance en la seguridad e integridad de los datos que nos permite tener la tecnología.

Desarrollo teórico de la sesión: 4 horas

ALGORITMOS DE CIFRADOS MODERNOS HECHOS CON SISTEMAS COMPUTACIONALES.

En la lección anterior se mencionaron algunos algoritmos de cifrado antiguos utilizados para ocultar información basados en la sustitución de caracteres, lamentablemente, estos algoritmos son bastante débiles e inseguros, poniendo en riesgo la integridad de la información al poder ser descifrados con fuerza bruta.

Una vez se halla el patrón de cifrado en estos algoritmos, son realmente fáciles de descifrar y obtener el texto real.

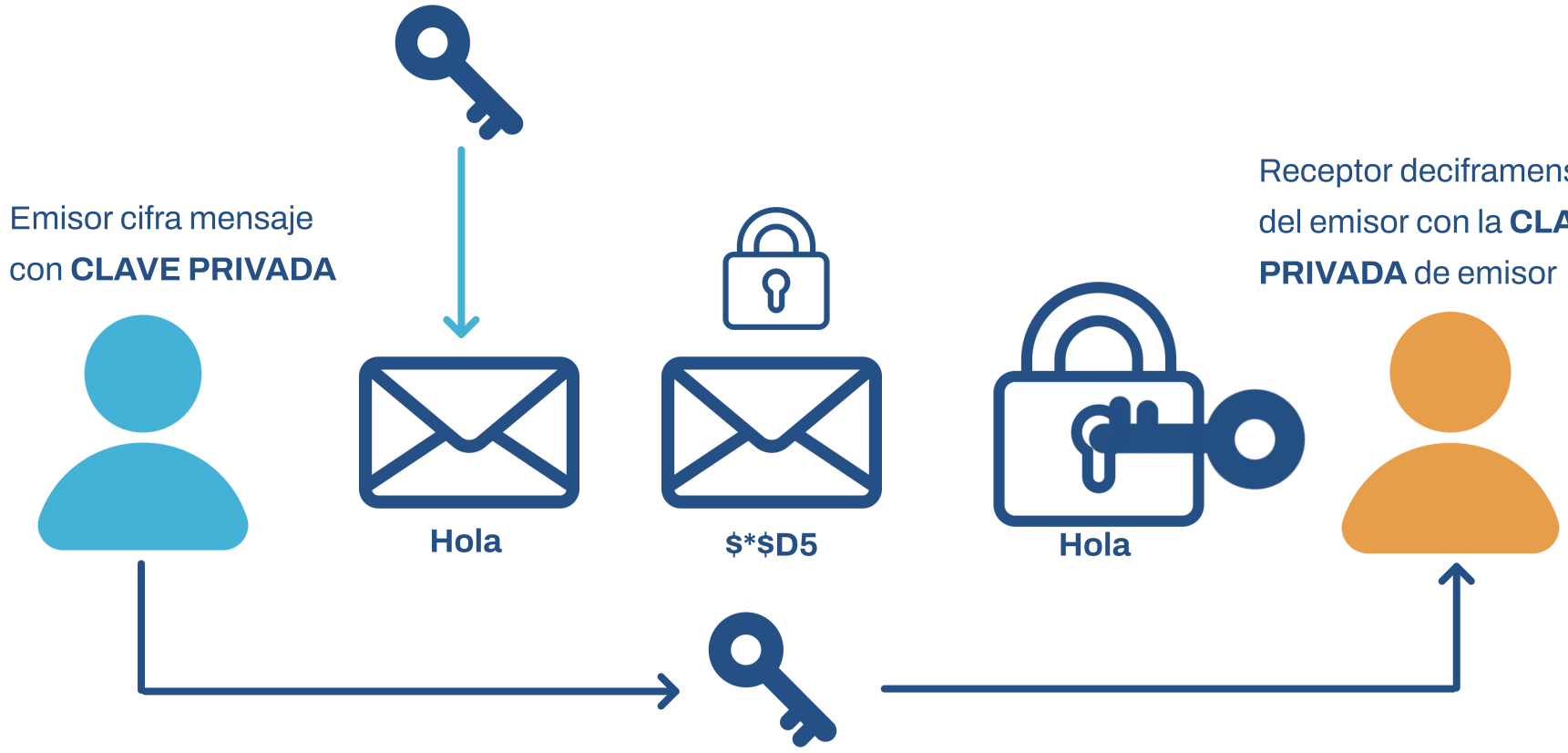
En el mundo moderno, contamos con el apoyo de la tecnología y la capacidad computacional para aumentar la seguridad de los archivos y textos que deseamos proteger, usando algoritmos altamente complejos que son imposibles de revertir a menos de que se tenga la autorización para hacer el descifrado.

Ahora nos vamos a adentrar en algunas de las tecnologías y los algoritmos de cifrado que se usan en la actualidad.

CRIPTOGRAFÍA DE CLAVE SIMÉTRICA

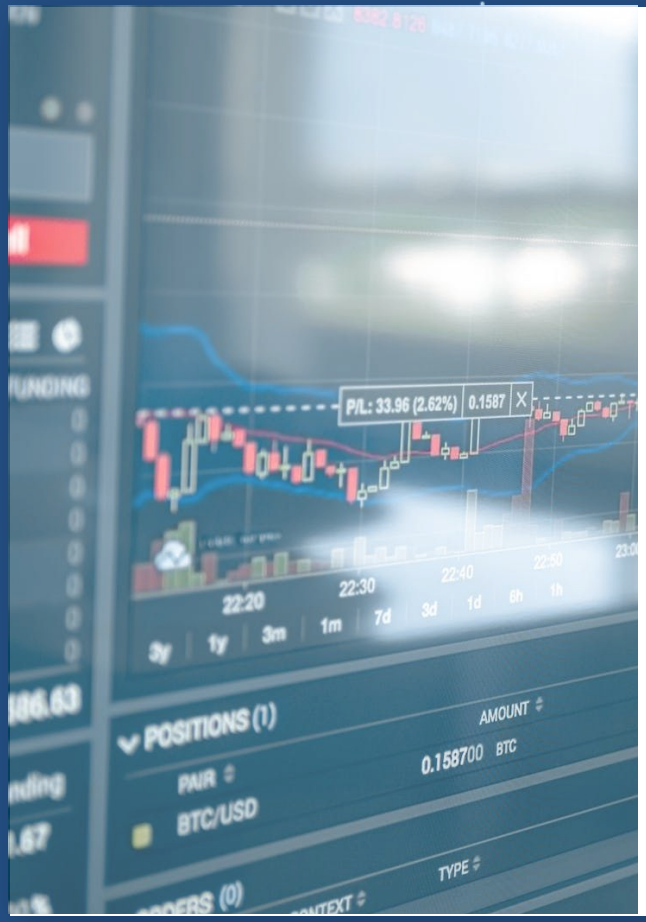
La criptografía de clave simétrica se refiere a los algoritmos criptográficos que emplean la misma clave tanto para cifrar como para descifrar datos, conocida como "clave simétrica" o "clave secreta". A diferencia de la criptografía de clave pública, donde las claves se generan en pares, y una clave realiza una transformación que solo puede revertirse con la otra clave, la clave simétrica ofrece seguridad y eficiencia cuando se utiliza adecuadamente. Estos algoritmos cifran datos bloque por bloque, siendo el tamaño del bloque establecido por el algoritmo (por ejemplo, AES utiliza bloques de 16 bytes). Es crucial seleccionar el modo adecuado, como CTR, CBC, o GCM, para cifrar mensajes más largos que el tamaño del bloque y garantizar la seguridad del cifrado subyacente.

+ info


Emisor cifra mensaje con **CLAVE PRIVADA**
Hola
$*$D5
Hola
Receptor deciframensaje del emisor con la **CLAVE PRIVADA** de emisor
Emisor envia su **CLAVE PRIVADA** a receptor

Como podemos ver en la ilustración, el emisor puede cifrar un mensaje con texto plano y enviar la llave para descifrarlo al emisor. ¿Qué sucede si el mensaje es interceptado? La respuesta es sencilla, quien intercepto el mensaje solo va a poder ver caracteres aleatorios que no tienen sentido, y no puede hacer un proceso inverso para llegar al texto plano original, ya que no existe un método para hacer ese procedimiento, podría llegar a cualquier texto si lo intentara. Descifrar el mensaje solo es posible para la persona que tenga la llave privada del emisor, de esta manera basta con hacer uso de ella y el mensaje va a aparecer en texto plano para el receptor.

Con este método de cifrado se puede garantizar la seguridad e integridad de la información que se envía a través de una red, aunque el archivo fuera interceptado por algún usuario malicioso solo va a tener un archivo inútil. Lo que se debe hacer es mantener en un sitio seguro la clave privada y solo compartirla con el usuario final o personas que necesitan tener acceso al contenido del archivo.



Criptografía de clave asimétrica.

La criptografía asimétrica, también llamada criptografía de clave pública o de dos claves, es un sistema criptográfico que utiliza dos claves interconectadas: una clave pública y una privada. Estas claves tienen roles complementarios, siendo la clave pública responsable del cifrado y la clave privada del descifrado. En el procedimiento, el destinatario genera ambas claves, compartiendo la clave pública con el emisor, quien tiene la opción de cifrar el mensaje. El mensaje cifrado solo puede descifrarse con la clave privada, asegurando que, si es interceptado, la información permanece oculta. Además, la generación única de esta pareja de claves garantiza la improbabilidad de que dos personas obtengan casualmente la misma pareja de claves.

En la criptografía asimétrica, al enviar un mensaje, se utiliza la clave pública del destinatario para cifrarlo, proporcionando confidencialidad ya que solo la clave privada del destinatario puede descifrarlo. Asimismo, utilizando la clave pública del destinatario, cualquiera puede cifrar mensajes que solo el destinatario puede descifrar con su clave privada. Si el propietario de las claves cifra un mensaje con su clave privada, cualquiera puede verificarlo usando la clave pública del remitente, permitiendo la identificación y autenticación del remitente, esencial en la firma digital. Los sistemas de clave pública eliminan la necesidad de acordar una clave compartida, ya que solo se requiere la clave pública del otro para comunicarse de manera segura.

+ info


Clave
distinta
Clave pública
Clave privada
Cifrado
Descifrado
Texto original
Datos codificados
Texto original

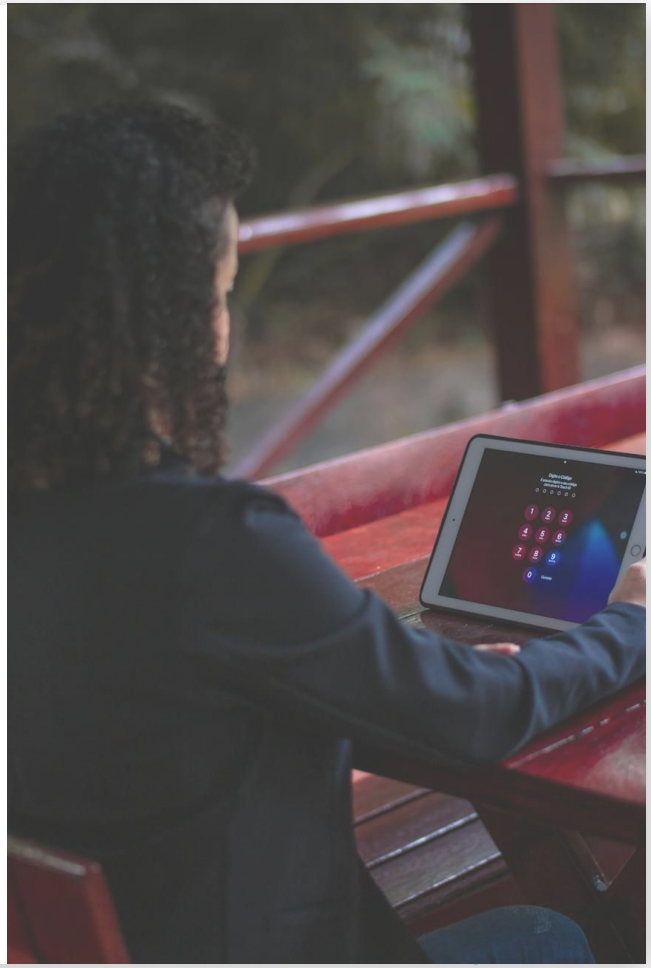
Cifrado híbrido.

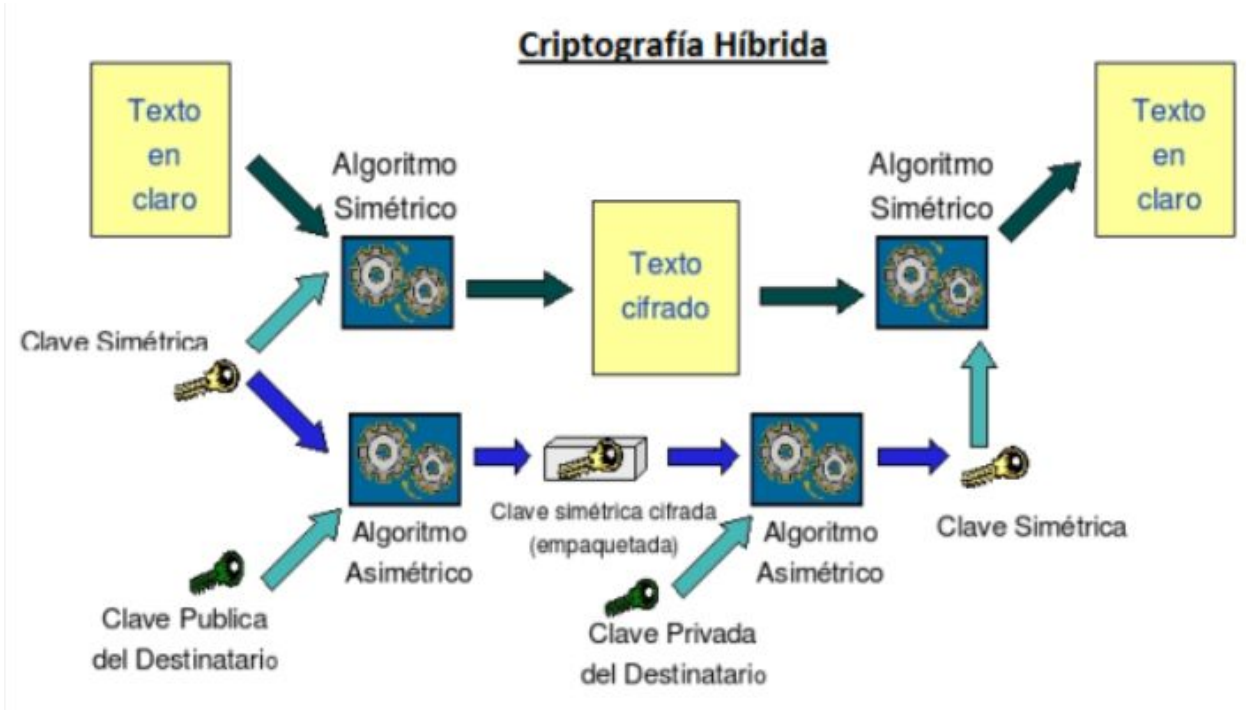
El cifrado híbrido es una técnica que combina la eficiencia de la criptografía de clave simétrica con la seguridad de la criptografía de clave pública. Esta estrategia se utiliza comúnmente en la práctica para abordar las limitaciones de ambos sistemas y aprovechar sus fortalezas respectivas. La criptografía simétrica destaca por su eficiencia en el cifrado y descifrado de grandes cantidades de datos. Sin embargo, enfrenta desafíos en el intercambio seguro de claves. Por otro lado, la criptografía asimétrica ofrece un intercambio seguro de claves mediante pares de claves pública y privada, pero su velocidad es inferior, especialmente para grandes volúmenes de datos.

El proceso de cifrado híbrido inicia con la generación de un par de claves pública y privada para cada usuario. Luego, para transmitir un mensaje, se crea una clave simétrica única para esa transacción, cifrando eficientemente el contenido del mensaje. Posteriormente, esta clave simétrica se cifra utilizando la clave pública del destinatario, asegurando así un intercambio seguro de claves. El mensaje cifrado simétricamente junto con la clave simétrica cifrada asimétricamente se envía al destinatario, quien, al descifrar la clave simétrica con su clave privada, puede descifrar el contenido del mensaje.

El cifrado híbrido ofrece eficiencia al aprovechar la criptografía simétrica para el cifrado de datos y, al mismo tiempo, garantiza la seguridad mediante la criptografía asimétrica para un intercambio seguro de claves.

+ info




Criptografía Híbrida
Texto en claro
Algoritmo Simétrico
Texto cifrado
Algoritmo Simétrico
Texto en claro
Clave Simétrica
Algoritmo Asimétrico
Clave simétrica cifrada (empaquetada)
Algoritmo Asimétrico
Clave Simétrica
Clave Publica del Destinatario
Clave Privada del Destinatario

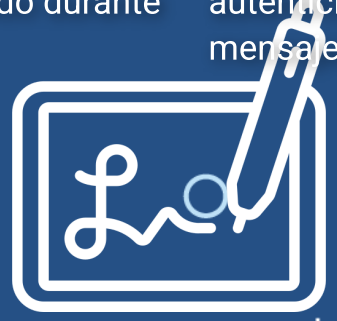
COLOMBIA POTENCIA DE LA VIDA

TIC

FIRMA DIGITAL

La firma digital es un componente esencial en la criptografía asimétrica, proporcionando autenticación y garantizando la integridad de mensajes electrónicos. Este mecanismo utiliza pares de claves públicas y privadas, donde el emisor genera una firma digital mediante su clave privada para adjuntarla al mensaje. La firma actúa como una huella única que verifica la identidad del remitente y asegura que el contenido del mensaje no ha sido alterado durante la transmisión.

Cuando un remitente decide firmar digitalmente un mensaje, se utiliza una función hash para crear un resumen único del contenido del mensaje. Luego, este resumen se cifra con la clave privada del remitente, generando la firma digital. La firma resultante se adjunta al mensaje original antes de enviarlo. El destinatario, al recibir el mensaje y la firma digital, puede verificar la autenticidad del remitente y la integridad del mensaje. Utilizando la clave pública del remitente, el destinatario descifra la firma digital y compara el resumen obtenido con un nuevo cálculo del resumen del mensaje recibido. Si ambos coinciden, se confirma la autenticidad del remitente y la integridad del mensaje.



Las firmas digitales son fundamentales en transacciones en línea, contratos electrónicos y comunicaciones seguras. En entornos empresariales y financieros, las firmas digitales aportan un nivel de seguridad adicional, permitiendo la verificación de la identidad de las partes involucradas y la garantía de la no manipulación de la información transmitida.

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

Código de Autenticación de Mensajes (MAC)

Un Código de Autenticación de Mensajes (MAC) funciona como la contraparte simétrica de una firma digital, donde dos o más partes comparten una clave común. En este proceso, una de las partes genera una etiqueta de MAC, que es esencialmente la versión simétrica de una firma digital, y la incorpora al documento. Posteriormente, cualquier otra parte puede verificar la integridad del mensaje utilizando la misma clave que se utilizó para crear la etiqueta de MAC. Es importante destacar que, dado que varias partes comparten la misma clave utilizada para generar las etiquetas de MAC, este método no es adecuado para autenticación o no repudio, ya que no se puede determinar claramente qué parte específica creó la etiqueta.

Hash en Criptografía

En criptografía, una función hash criptográfica desempeña el papel de convertir datos arbitrarios en una "huella digital" de longitud fija. Estas funciones están diseñadas con la dificultad de encontrar dos entradas diferentes que produzcan la misma huella digital, y es igualmente complicado hallar un mensaje cuya huella coincida con un valor predefinido.

A diferencia de los esquemas de cifrado, las funciones hash no requieren una clave específica. Cualquier persona puede calcular el hash de una entrada dada, y la función hash siempre generará la misma salida para la misma entrada. Estas funciones hash son esenciales en diversos algoritmos y protocolos criptográficos, incluyendo algoritmos de firma digital, ciertos algoritmos MAC, así como en protocolos de autenticación y almacenamiento de contraseñas. Su utilidad se extiende a lo largo de diversos ámbitos de la criptografía.