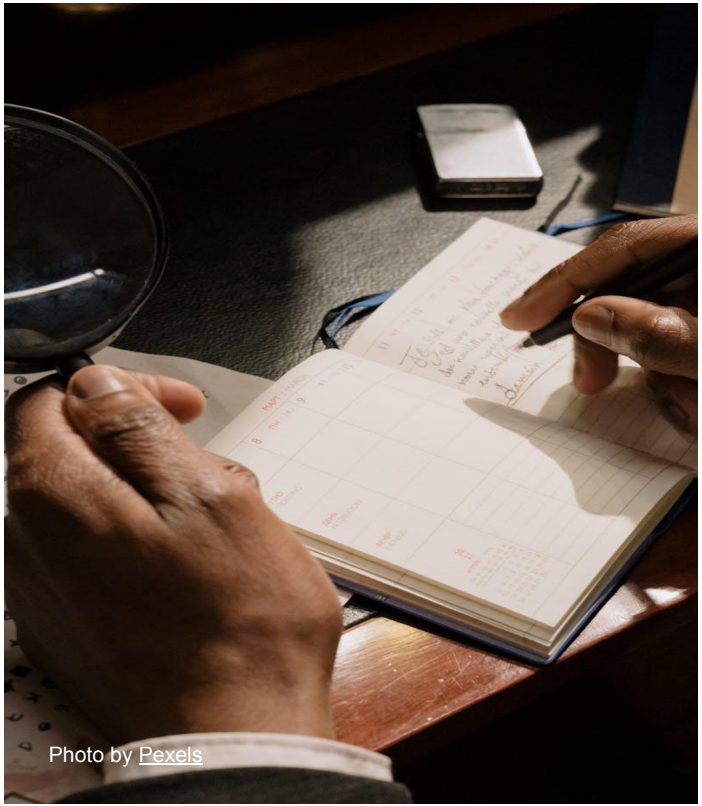
Conceptos básicos de criptografía

Comprender los fundamentos del cifrado

Introducción a la criptografía



Comunicación segura a través de códigos

- La criptografía es la ciencia de cifrar y descifrar información para mantenerla segura.
- Implica el uso de códigos y cifrados para ocultar mensajes a partes no autorizadas.
- Antes de que los datos se codifiquen, se denominan texto plano. Un algoritmo criptográfico se utiliza para cifrar el mensaje de texto plano y producir un mensaje de texto cifrado y descifrar el texto cifrado a su texto plano original. Todos los algoritmos criptográficos se basan en claves (es decir, un número binario) para mantener su seguridad.
- Cada algoritmo tiene un espacio de claves específico de valores que son válidos como clave para un algoritmo específico definido por su tamaño en bits o longitud.

Tipos de criptografía

1. La criptografía simétrica utiliza una única clave para el cifrado y descifrado.

2. La criptografía asimétrica implica el uso de pares de claves: claves públicas y privadas.

3. Ambos tipos desempeñan papeles cruciales para garantizar la seguridad y privacidad de los datos.

Conceptos básicos del cifrado simétrico

Eficiente y seguro

- El cifrado simétrico es eficaz para grandes cantidades de datos.
- Utiliza una única clave para los procesos de cifrado y descifrado.
- Método rápido y seguro para proteger información confidencial.

Cuestiones clave de gestión

- La distribución de claves puede ser un desafío para la implementación a gran escala.
- Si la clave se ve comprometida, todos los datos cifrados con ella están en riesgo.
- No proporciona autenticación del remitente ni no repudio.

Cifrado asimétrico

Comunicación segura

- El cifrado asimétrico proporciona un medio de comunicación seguro mediante el uso de dos claves diferentes para el cifrado y descifrado.
- La clave pública se puede distribuir libremente, lo que permite a cualquiera enviar mensajes cifrados al destinatario.
- Es muy seguro ya que la clave privada se mantiene en secreto y no se comparte con nadie.

Complejidad y riesgo

- El cifrado asimétrico puede ser más lento en comparación con el cifrado simétrico debido a la complejidad de utilizar dos claves.
- El proceso de generación y gestión de pares de claves puede resultar engorroso y requiere un manejo cuidadoso para evitar violaciones de seguridad.
- Puede existir el riesgo de que la clave privada se vea comprometida si no se implementan las medidas de seguridad adecuadas.

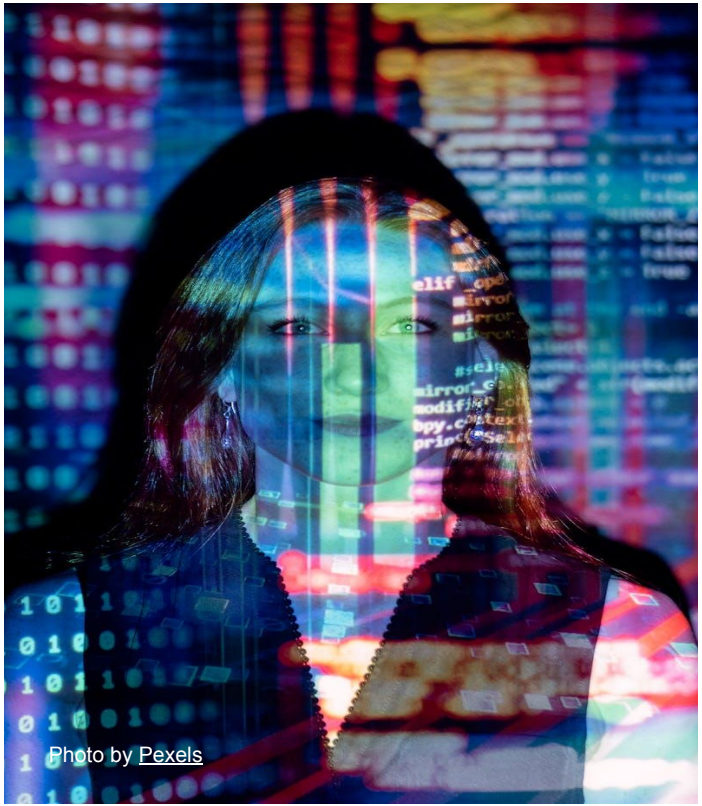
Firmas digitales

Verificar integridad

- La firma digital es un mecanismo electrónico que permite demostrar que un mensaje ha sido enviado por un usuario concreto (es decir, que no ha sido repudiado) y que no ha sufrido modificaciones durante su transmisión (integridad).
- Las firmas digitales proporcionan una forma de verificar la autenticidad de un mensaje digital.
- Mediante el uso de técnicas criptográficas, las firmas digitales garantizan la integridad del documento.
- Las firmas digitales funcionan mediante un algoritmo hash y una criptografía asimétrica de clave pública.

Photo by Pexels

Huellas digitales: garantizar la integridad de los datos



Funciones hash

- El hashing es un tipo de criptografía que no es un algoritmo de cifrado. En su lugar, el hashing se utiliza para producir un identificador o representación única -conocido como valor hash, hash, suma de comprobación, código de autenticación de mensajes (MAC), huella dactilar, huella digital o compendio - de los datos.
- Las funciones hash generan huellas digitales únicas para la verificación de datos.
- Son esenciales para garantizar la integridad de los datos y las medidas de seguridad.

PKI: una forma segura de gestionar certificados digitales

1. La infraestructura de clave pública proporciona un marco para la gestión segura de certificados digitales.

2. PKI garantiza la autenticidad, integridad y confidencialidad de los certificados digitales.

3. Utiliza una combinación de claves criptográficas públicas y privadas para una comunicación segura.

Criptoanálisis

Descifrar código

- El criptoanálisis implica descifrar códigos y cifrados para descifrar mensajes secretos.
- Las técnicas incluyen análisis de frecuencia, ataques de fuerza bruta y criptoanálisis.

Criptografía: seguridad de las comunicaciones

Herramienta de seguridad esencial

La criptografía desempeña un papel crucial a la hora de proteger los datos del acceso no autorizado y garantizar la privacidad.

Técnicas de encriptación

Se utilizan varios algoritmos de cifrado como RSA, AES y DES para proteger los canales de comunicación.

Firmas digitales

Las firmas digitales autentican al remitente y garantizan la integridad de los datos en las comunicaciones digitales.