Clase 3: Soluciones criptográficas

¿Qué es la criptografía?

La criptografía es un elemento clave de la ciberseguridad. Consiste en el estudio de técnicas de comunicaciones seguras, donde se codifica el texto ordinario para convertirlo en texto cifrado, y luego se vuelve a convertir en texto ordinario cuando llega a su destino.

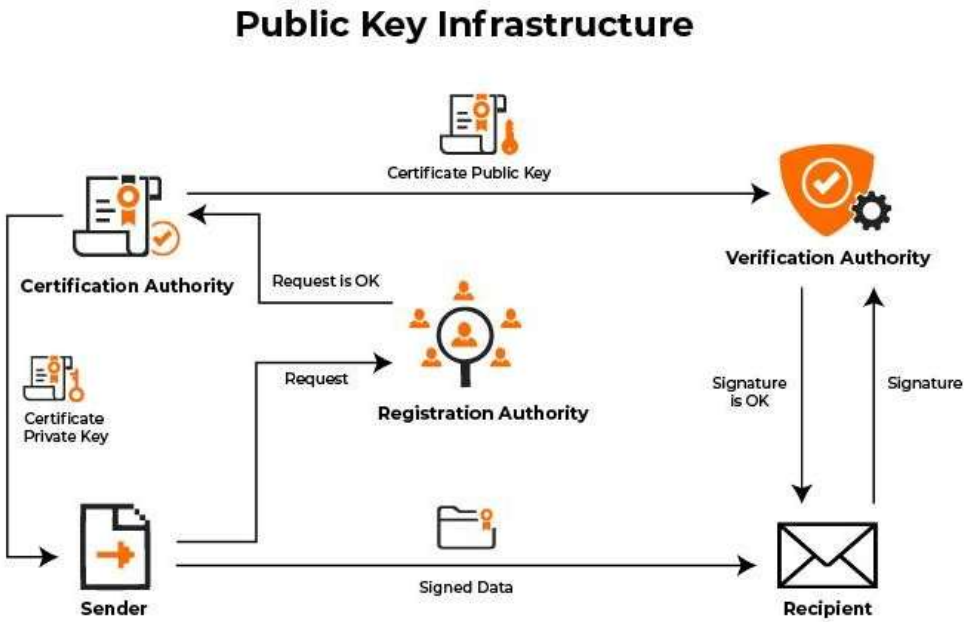
La palabra criptografía proviene de dos términos griegos: "kryptós", que significa oculto, y "graphein", que significa escribir, por lo que literalmente se traduce como escritura oculta.

Infraestructura de llave pública

La infraestructura de llave pública consiste en una serie de tecnologías y políticas para la creación y uso de certificados digitales.

Provee:

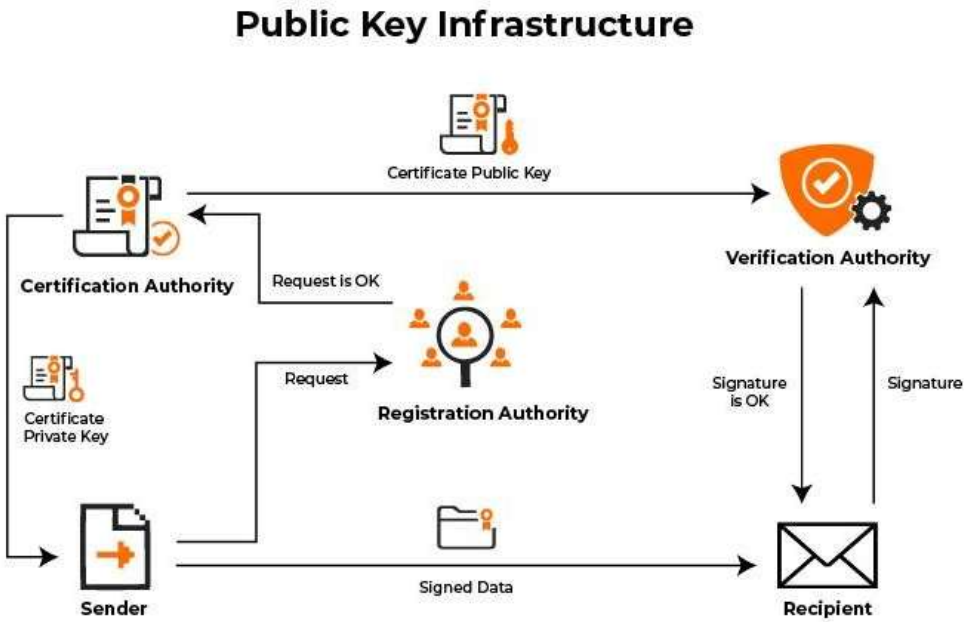
- Autenticación de identidad
- Verificación de integridad
- Garantía de privacidad
- Autorización de acceso
- Autorización de transacciones
- Soporte de no-repudio



Infraestructura de llave pública

Llave privada (private key) y llave pública (public key): sistema de cifrado asimétrico utilizado para generar y validar certificados a través de autoridad certificadora (*Certificate Authority*, CA). También se utiliza como medio de autenticación para inicios de sesión o descifrado de datos.

Custodia de claves (key escrow): ocurre cuando la autoridad certificadora mantiene una copia de la llave privada de un usuario. Esto no es una solución muy favorable.



Control de entendimiento

Práctica

Llave privada y llave pública en servidor Linux

Control de entendimiento

El sistema de llave privada y llave pública puede ser utilizado como método de autenticación

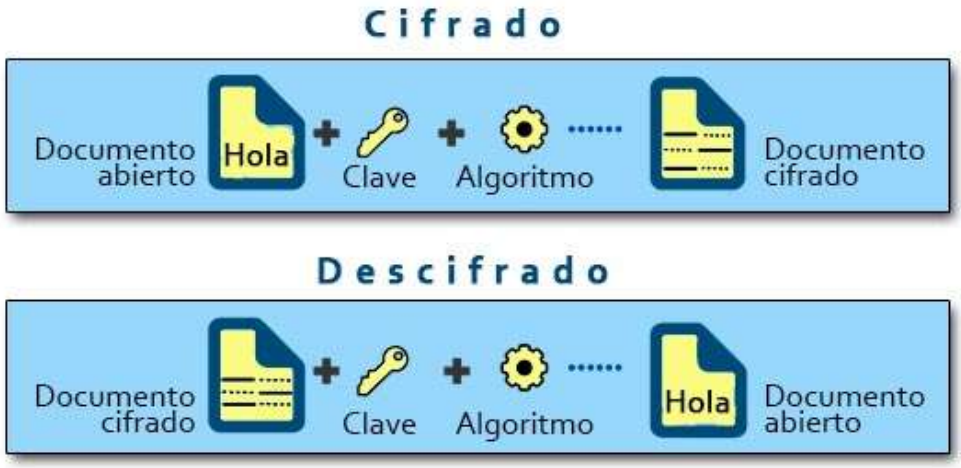
Verdadero

Cifrado

El cifrado permite codificar la información de tal forma que no sea entendible sin tener la llave para decodificarla.

El proceso de cifrado/encriptación está basado en dos principios:

- **Confusión:** el texto plano debe ser cambiado significativamente en el texto cifrado.
- **Difusión:** si el texto plano es cambiado, sin importar qué tan pequeño sea el cambio, debe cambiar al menos la mitad del texto cifrado resultante.



Cifrado - Niveles

Disco completo: beneficioso si el disco es robado o accedido por alguien no debido, es muy probable que la información no pueda ser extraída. Ejemplo: BitLocker

Partición: importante si solamente se quiere cifrar una parte del disco.

Volumen: parecido al cifrado de partición, con la diferencia que funciona a nivel del sistema de archivos.

Archivo: de las más utilizadas. Cifra solamente un archivo.

Base de datos: no es posible acceder a la información desde el archivo donde se guarda.

Transporte/Comunicación: utilizado para cifrar información transmitida en una comunicación. Ejemplo: SSL/TLS, SSH

Control de entendimiento

¿Cuáles son los principios en los que se basa el cifrado?

Confusión y difusión

Algoritmos criptográficos

Utilizados para cifrar la información. Dependiendo del tipo, puede utilizar llaves predefinidas o matemáticamente relacionadas.

Los algoritmos de cifrado se basan en:

- **Fuerza de llave (key strength):** depende de la entropía de la llave, o sea qué tan única es.
- **Expansión de llave (key stretching):** qué tan larga será la llave generada.
- **Intercambio de llaves:** la llave debe ser transmitida en cierta forma.

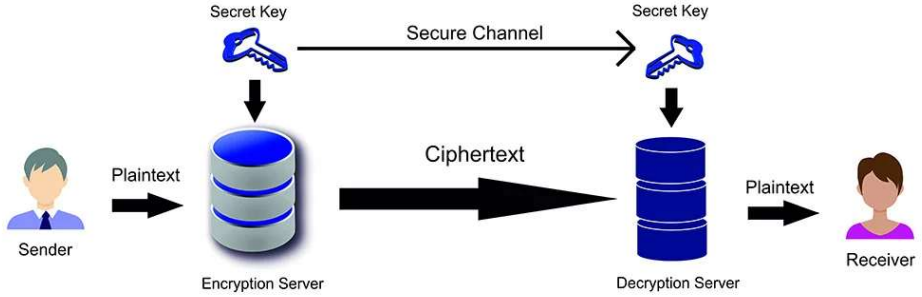
Según el tipo, los algoritmos de cifrado pueden ser:

Simétricos: utilizan una llave común compartida entre el emisor y el receptor. Una analogía puede ser una caja fuerte, la misma llave tienen que tenerla todas las partes.

Asimétricos: consta de llave privada y llave pública. La llave pública del receptor se comparte para que se utilice en la encripción en conjunto con la llave privada del emisor.

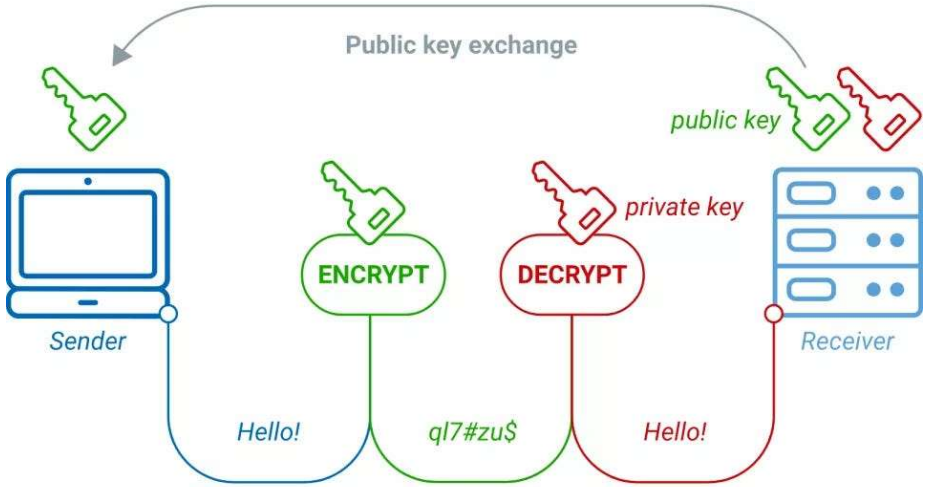
Algoritmos criptográficos

Cifrado simétrico



Symmetric Cryptography

Cifrado asimétrico



Control de entendimiento

¿La “fuerza de llave” se refiere a qué tan única es una llave?

Afirmativo

Control de entendimiento

¿El cifrado simétrico utiliza una llave compartida entre el emisor y el receptor?

Verdadero

Herramientas para cifrado

Módulo de Plataforma Confiable (*Trusted Platform Module, TPM*): chip incrustado que provee el almacenamiento de llaves, contraseñas y certificados digitales.

Módulo de Seguridad de Hardware (*Hardware Security Module, HSM*): usados para almacenar claves, y evitar que sean corrompidos. Son extraíbles, a diferencia de los TPM que son incrustados.

Sistema de Gestión de Claves (*Key Management System, KMS*): software utilizado para almacenar llaves privadas en un sistema. Es un "mal necesario" muchas veces.

Enclave seguro (*Secure Enclave*): parecido a los TPM, pero son utilizados para sistemas operativos de dispositivos móviles, como Android y iOS.

Herramientas para cifrado

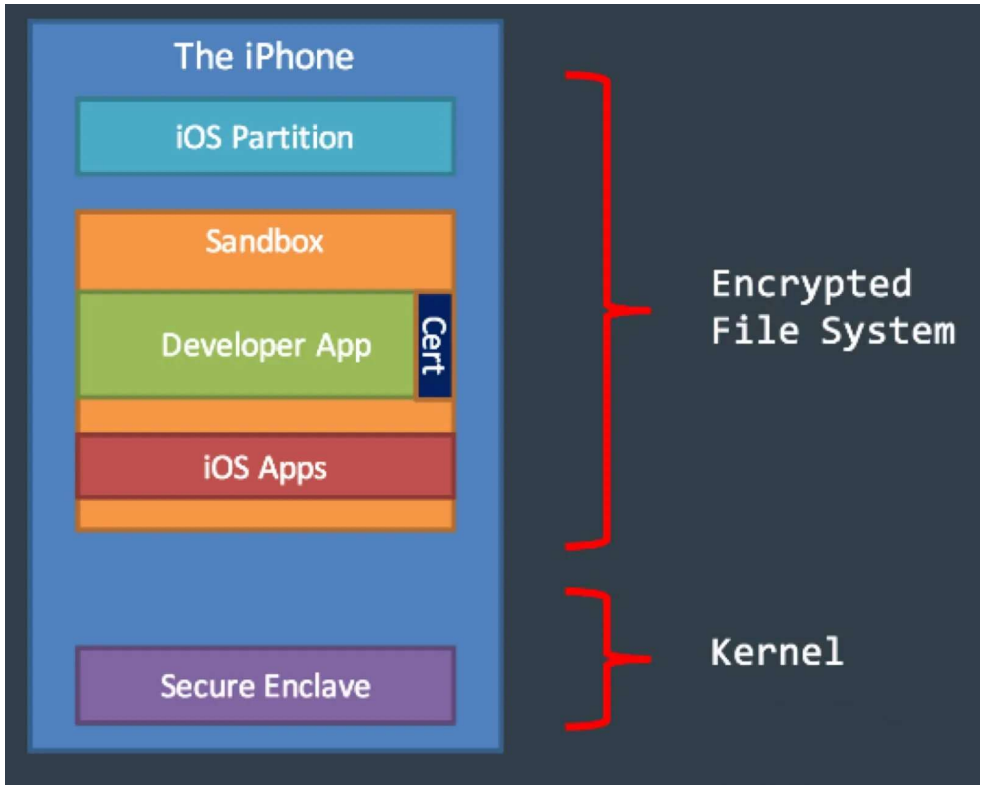
TPM

HSM

Herramientas para cifrado

KMS

Enclave seguro



Control de entendimiento

¿Cuál de las herramientas para cifrado es extraíble?

Módulo de seguridad de hardware (*Hardware Security Module*, HSM)

Ofuscación

Dentro del entorno de la comunicación o del lenguaje, la ofuscación u ofuscamiento (en inglés: *Obfuscation*) , es el oscurecimiento del significado previsto de una comunicación haciendo que el mensaje sea difícil de entender, generalmente con un lenguaje confuso y ambiguo.

Original Source Code Before Control Flow Obfuscation

```
public int CompareTo (Object o) {
    int n = occurrences -
    ((WordOccurrence)o) .occurrences ;
    if (n == 0)  {
        n = String.Compare
  (word, ((WordOccurrence)o) .word) ;
    }
    return (n) ;
}
```

Reverse-Engineered Source Code After Control Flow Obfuscation

```
private virtual int _a(Object A+0) {
    int local0 ;
    int local1 ;
    local 10 = this.a - (c)  A_0.a;
    if (local10  != 0) goto i0 ;
    while  (true)  {
        return local1;
    }
    i1: local10 =
System.String.Compare(this.b,  (c)
A_0.b) ;
    goto  i0;
}
```

Ofuscación – Tipos

Tokenización: asigna un valor sustituto aleatorio, sin relación matemática, que permanece enlazado con el valor original. Puede o no preservar el formato original.

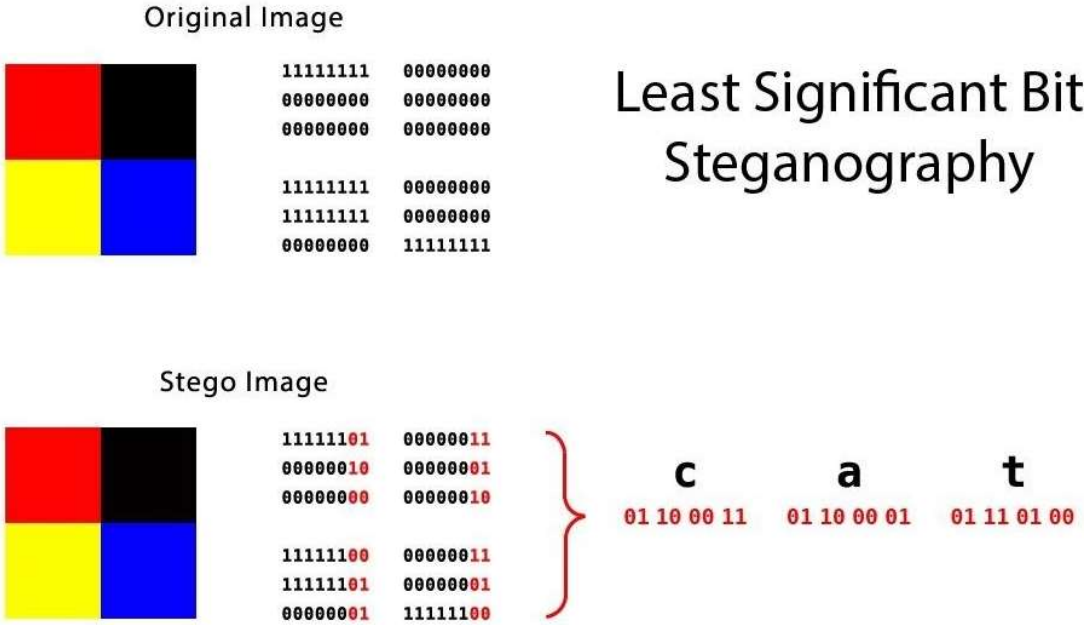
Enmascaramiento de datos: se remueve información personal o sensible, pero mantiene información usable. Ideal para ambientes de desarrollo.

Redacción: se sustituyen caracteres de los datos por un caracter cualquiera (como *), con el fin de ocultar la información.

Encrypted Values	Token Values
O/Mw+qmQITMzIZSz/ V5cje5rCwlWU8hMzM+=	6389 7207 2518 0518 Tbr Tfeilsia
Redacted Values	**Masked Values**
**** ***** **** 9313 Eli *****	2223 0167 2837 2736 John Andreadis

Ofuscación – Tipos

Esteganografía (*Steganography*): involucra esconder mensajes para que personas ajenas no sepan que hay un mensaje a simple vista. Los datos se esconden en archivos de audio, video, imágenes u otros, utilizando bits que no afecten mucho el archivo original.



Control de entendimiento

Práctica

Esteganografía

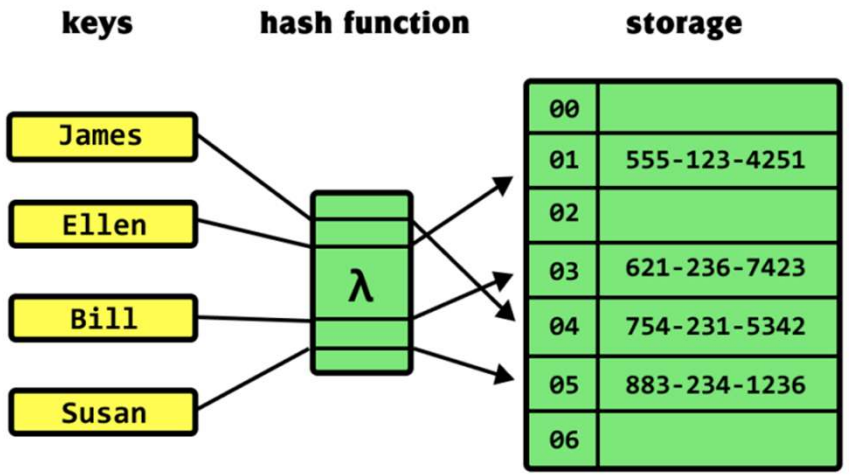
Control de entendimiento

¿En el método de ofuscación conocido como “tokenización” se cambian los caracteres por un caracter cualquiera (como *)?

Falso

Hashing y salting

Hashing: un hash es un resumen generado por una regla matemática y algoritmo utilizado comúnmente como "huella digital" para verificar la integridad de archivos y mensajes. Solo funciona generándolo, no se puede descifrar ya que no está cifrado con una llave.



Salting (condimentar): dato añadido a un valor para que el hash computado sea completamente distinto. Sirve como medida de seguridad ante ataques que utilizan o precalculan hashes.

Password	p4s5w3rdz	p4s5w3rdz	p4s5w3rdz	p4s5w3rdz
Salt	-	-	et52ed	ye5sf8
Hash	f4c31aa	f4c31aa	lvn49sa	z32i6t0

Control de entendimiento

Práctica

Hashing y salting

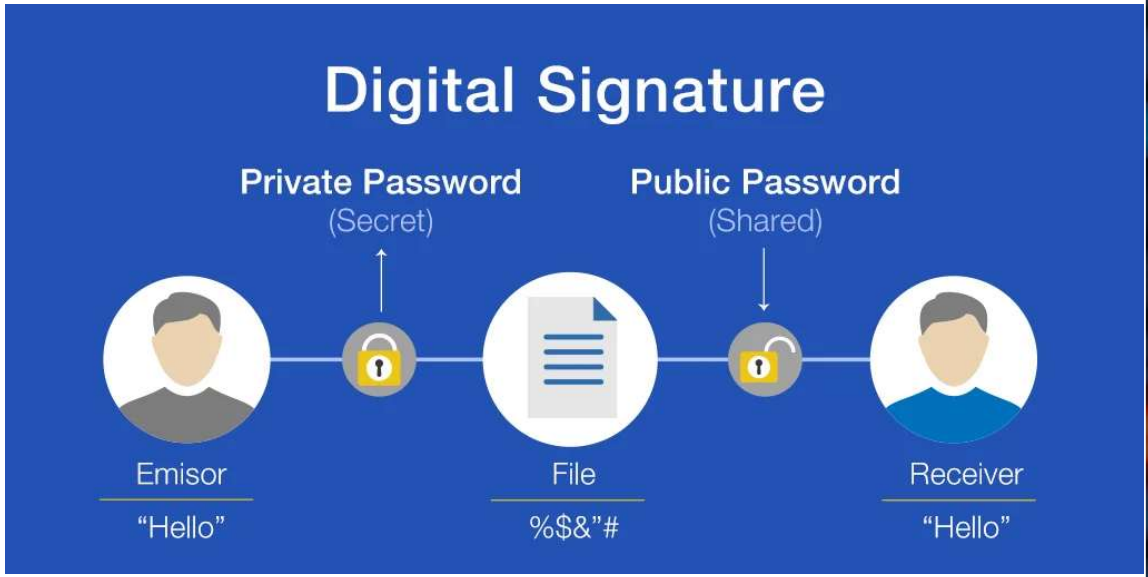
Control de entendimiento

¿El “salting” se utiliza como medida de seguridad?

Verdadero

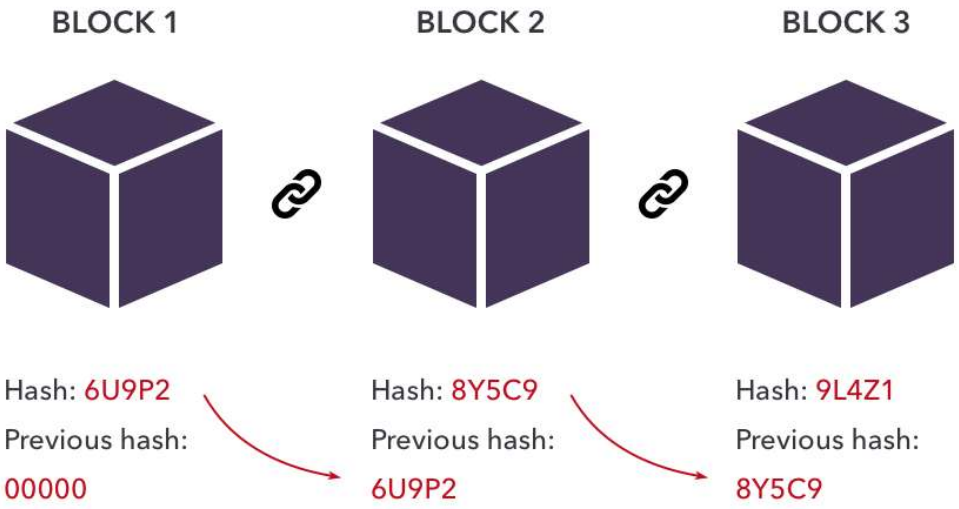
Firmas digitales

Las firmas digitales son un recurso para proveer integridad y autenticación, ya que se utiliza la llave privada del emisor y la llave pública del receptor para firmar el mensaje o archivo.
Adicionalmente, las firmas digitales proveen no-repudio, ya que se sabe con exactitud quién fue el emisor y quién el receptor.



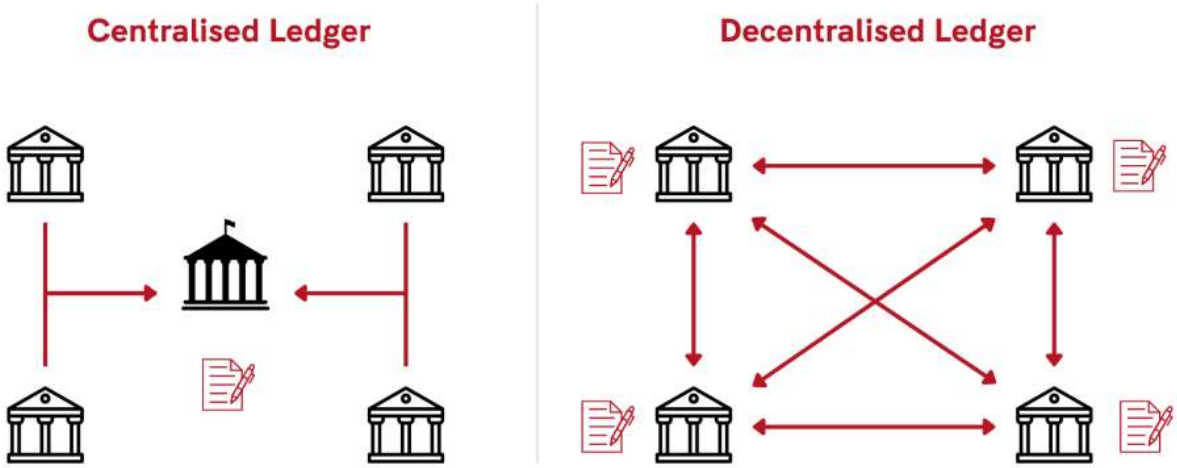
Blockchain

Blockchain (cadena de bloques) es un sistema para gestionar transacciones compartidas en una misma red. Dichas transacciones están agrupadas en bloques, y cada una está relacionada con la anterior por medio de un hash.
Mayormente conocido por su uso relacionado con las criptomonedas.



Libro de contable de acceso público (Open public ledger)

Dentro del blockchain se utilizan ledgers (libros contables), que son una lista de las transacciones realizadas en una red. Este tipo de libros son descentralizados, lo que significa que cualquier persona puede accederlos. Para proteger la privacidad, se utiliza un alias para cada usuario que realiza la transacción.



Control de entendimiento

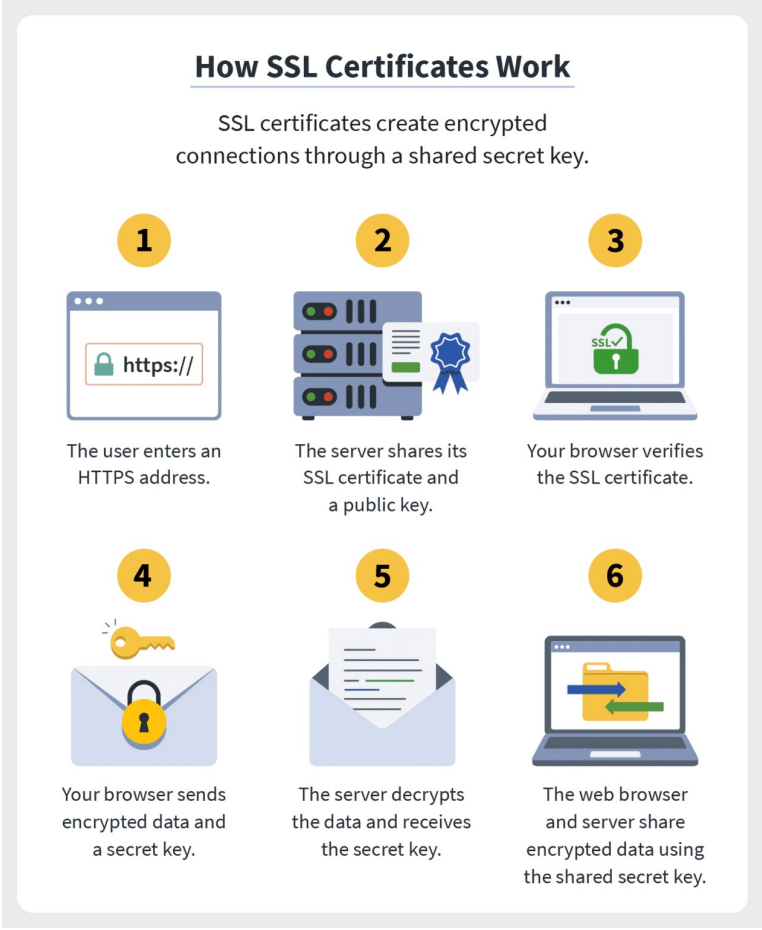
¿El certificado digital ayuda a proveer no-repudio?

Verdadero

Certificado digital

Un certificado digital es un **bloque de datos firmado digitalmente**, el cual permite utilizar criptografía de llave pública para **propósitos de identificación**. Estos certificados son generados por una autoridad certificadora (*Certificate Authority,* CA).

El uso más común es en los certificados SSL/TLS, utilizados en los sitios web.



Certificado digital - Elementos relacionados

Autoridad certificadora (*Certificate Authority*, CA): entidad confiable encargada de generar certificados digitales y validar al portador del certificado. Puede ser interna o externa a la organización.

Lista de revocación de certificados (*Certificate Revocation List*, CRL): mecanismo utilizado para distribuir información acerca de la revocación de certificados y verificar la validez de un certificado.

Protocolo de estado de certificado en línea (*Online Certificate Status Protocol*, OCSP): es un mecanismo reciente para identificar la revocación de certificados en tiempo real, en lugar de depender de tener una CRL actualizada.

Certificados auto-firmados (*Self-signed certificates*): los certificados auto-firmados (no generados por una CA) son utilizados comúnmente para propósitos de desarrollo, donde la confianza no es un problema.

Certificado digital - Elementos relacionados

Generación de solicitud de firma de certificado (*Certificate Signing Request*, CSR): para que un certificado digital sea generado, se debe enviar una solicitud, junto con información como FQDN, nombre de la organización, departamento, u otra información.

Certificado comodín (*Wildcard certificate*): es un certificado generado para ser utilizado por cualquier cantidad de subdominios para un solo dominio registrado. Ejemplo: **.usonsonate.edu.sv*.

Control de entendimiento

¿Un certificado “wildcard” permite ser utilizado por un máximo de 10 subdominios?

Falso

Control de entendimiento

¿Un certificado auto-firmado es utilizado comúnmente en entornos de producción?

Falso

Control de entendimiento

Práctica

Captura con Wireshark de HTTP y HTTPS

Control de entendimiento

Práctica

Obtención de información de certificado SSL con SSLyze/SSLscan

Lectura asignada

A partir de la lectura del capítulo 3 del libro “Criptografía Esencial: …”, responda la siguiente pregunta en el foro de Sinapsis utilizando sus propias palabras:

¿Qué problema resolvió la criptografía asimétrica?