TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLÓGICO DE TLAXIACO

SEGURIDAD Y VIRTUALIZACIÓN

INVESTIGACIÓN

Práctica 1

CARRERA:

INGENIERIA EN SISTEMAS COMPUTACIONALES

INTEGRANTES DEL EQUIPO:

Sandra Gabriela Velasco Guzmán

Amilkar Vladimir Reyes Reyes

Rael Gabriel Bautista

Arnol Jesus Cruz Ortiz

DOCENTE

OSORIO SALINAS EDWARD

Fecha de entrega: 30 agosto 2024

Tlaxiaco, Oax., 29 de agosto de 2024.

"Educación, ciencia y tecnología, progreso día con día"®

Tabla de contenido

Conceptos

1. Contraseña

Definición: Una secuencia de caracteres (letras, números, símbolos) utilizada para verificar la identidad de un usuario o para acceder a recursos protegidos.

Características:

Seguridad: Debe ser única, compleja y difícil de adivinar para proteger efectivamente las cuentas.

Mejores Prácticas: Uso de combinaciones alfanuméricas, longitud mínima, cambio regular, y evitar palabras comunes.

2. Certificado Digital

Definición: Un archivo electrónico que utiliza criptografía para verificar la identidad de una entidad (como una persona o una organización) y establecer una conexión segura.

Componentes:

Clave Pública: Parte del certificado que se utiliza para cifrar datos y verificar firmas digitales.

Clave Privada: Parte secreta que se usa para descifrar datos y firmar digitalmente.

Autoridad de Certificación (CA): Entidad que emite y gestiona los certificados digitales.

Uso: Asegurar comunicaciones en línea, firmar documentos y autenticar identidades.

3. Firma Digital

Definición: Un mecanismo criptográfico que permite verificar la autenticidad e integridad de un mensaje o documento digital.

Funcionamiento:

Generación: Se utiliza una clave privada para firmar el documento.

Verificación: La firma se verifica utilizando la clave pública correspondiente.

Propósito: Garantizar que el documento no haya sido alterado y confirmar la identidad del firmante.

4. Cifrado Simétrico

Definición: Un método de cifrado en el que la misma clave se usa tanto para cifrar como para descifrar la información.

Ejemplos: AES (Advanced Encryption Standard), DES (Data Encryption Standard).

Ventajas:

Rápido y eficiente: Menor carga computacional.

Desventajas:

Distribución de claves: La clave debe ser compartida de manera segura entre las partes.

5. Cifrado Asimétrico
Definición: Un método de cifrado que utiliza un par de claves relacionadas: una clave pública y una clave privada.

Funcionamiento:

Clave Pública: Se usa para cifrar datos y se puede compartir abiertamente.

Clave Privada: Se usa para descifrar datos y debe ser mantenida en secreto.

Ejemplos: RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography).

Ventajas:

Seguridad: La clave privada no necesita ser compartida.

Desventajas:

Más lento: Generalmente más lento que el cifrado simétrico.

6. Encriptación
Definición: Proceso de convertir datos o información en un formato codificado que solo puede ser leído o entendido por personas autorizadas, utilizando algoritmos de cifrado.

Sinónimos: Cifrado.

Objetivo: Proteger la confidencialidad e integridad de la información durante el almacenamiento o la transmisión.

Ejemplos y Aplicaciones

Contraseñas: Acceso a sistemas y aplicaciones.

Certificados Digitales: HTTPS para sitios web seguros.

Firma Digital: Documentos legales y contratos electrónicos.

Cifrado Simétrico: Protege datos en reposo, como archivos en un disco.

Cifrado Asimétrico: Correos electrónicos seguros, intercambio de claves.

Encriptación: Protección general de datos durante la transmisión y almacenamiento.

Algoritmos de Cifrado

1. AES (Advanced Encryption Standard)
Definición: AES es un algoritmo de cifrado simétrico de bloque que es ampliamente utilizado para proteger datos. Fue adoptado como estándar por el Instituto Nacional de Estándares y Tecnología (NIST) en 2001.

Características:

Tamaño de Clave: Soporta claves de 128, 192 y 256 bits.

Modo de Operación: Funciona con bloques de 128 bits, y puede utilizar varios modos de operación (como CBC, GCM, etc.) para mejorar la seguridad y la funcionalidad.

Seguridad: AES se considera muy seguro y eficiente. Es resistente a ataques conocidos como el ataque de fuerza bruta.

Uso: Se utiliza en aplicaciones como la protección de datos en tránsito (por ejemplo, en conexiones VPN) y datos en reposo (por ejemplo, en discos duros cifrados).

2. SHA-256 (Secure Hash Algorithm 256-bit)
Definición: SHA-256 es una función de hash criptográfica que produce un valor de 256 bits (32 bytes) a partir de cualquier entrada de datos. Es parte de la familia de algoritmos SHA-2.

Características:

Unidireccional: No se puede revertir el hash para obtener los datos originales.

Seguridad: Diseñado para ser resistente a colisiones (dificultad para encontrar dos entradas diferentes que produzcan el mismo hash) y preimagen (dificultad para deducir la entrada a partir del hash).

Uso: Se usa en la integridad de datos y en la firma digital. Es común en criptomonedas como Bitcoin para asegurar transacciones y en la autenticación de archivos.

3. Sociedad Anónima
Definición: "Sociedad Anónima" no es un algoritmo de cifrado ni un término relacionado con criptografía. Es un tipo de entidad jurídica en muchos países, similar a una "Sociedad Anónima" o "Corporación" en el ámbito corporativo. Si te referías a un término diferente relacionado con cifrado, por favor, proporciona más detalles.

Estándares de Cifrado

1. SSL (Secure Sockets Layer)

Definición: SSL es un protocolo de seguridad desarrollado por Netscape para cifrar datos transmitidos a través de redes, como Internet. Es la predecesora de TLS.

Características:

Propósito: Asegura la comunicación entre un navegador web y un servidor.

Versiones: SSL 1.0, 2.0 y 3.0. Las versiones 2.0 y 3.0 tienen vulnerabilidades y ya no se consideran seguras.

Uso: Aunque SSL ha sido reemplazado por TLS, muchos todavía se refieren a SSL en contextos de cifrado de comunicaciones.

2. TLS (Transport Layer Security)

Definición: TLS es el sucesor de SSL y es un protocolo de seguridad que asegura la comunicación en redes, como Internet. TLS 1.0 fue basado en SSL 3.0.

Características:

Versiones: TLS 1.0, 1.1, 1.2 y 1.3. Cada versión ha mejorado la seguridad y la eficiencia sobre la anterior.

Propósito: Cifra la comunicación para proteger la privacidad e integridad de los datos durante la transmisión.

Uso: TLS es ampliamente utilizado en conexiones HTTPS para asegurar sitios web y en otros protocolos de red que requieren cifrado.

Protocolos de Seguridad

1. HTTPS (Hypertext Transfer Protocol Secure)
Definición: HTTPS es una extensión del protocolo HTTP que utiliza TLS/SSL para cifrar la comunicación entre un navegador web y un servidor web.

Características:

Cifrado: Protege la confidencialidad e integridad de los datos durante la transmisión.

Autenticación: Verifica la identidad del servidor mediante certificados digitales.

Uso: Es común en sitios web que requieren seguridad, como servicios bancarios en línea y tiendas de comercio electrónico.

2. SFTP (SSH File Transfer Protocol)
Definición: SFTP es un protocolo de red que proporciona un acceso seguro a la transferencia de archivos y a la gestión de archivos en sistemas remotos.

Características:

Basado en SSH: Utiliza el protocolo SSH para cifrar las transferencias de archivos y las operaciones de gestión.

Seguridad: Protege contra la interceptación y manipulación de datos durante la transferencia.

Uso: Ideal para transferencias seguras de archivos en entornos corporativos y servidores remotos.

3. SSH (Secure Shell)
Definición: SSH es un protocolo de red para operar servicios de red de manera segura sobre una red insegura. Proporciona una interfaz segura para acceder y administrar sistemas remotos.

Características:

Cifrado: Cifra toda la comunicación entre el cliente y el servidor para proteger contra espionaje y ataques.

Autenticación: Utiliza autenticación basada en claves públicas o contraseñas.

Uso: Se utiliza comúnmente para administración remota de sistemas, transferencia segura de archivos (SFTP) y túneles seguros para otras aplicaciones.