Usando Criptografía

Descargar estos apuntes

Índice

Objetivos

- Comprender los conceptos básicos del cifrado de datos y aplicarlos.
- Comprender cómo los certificados y las firmas digitales garantizan la autenticidad, integridad y no repudio de las comunicaciones digitales aplicándolos.

Descripción de la tarea

Cifrado simétrico

Usa el comando gpg (de GnuPG) para cifrar y descifrar un mensaje de forma simétrica

1. Crea un nuevo documento que contenga algún texto y nombrarlo `simetrico` (sin extensión).
2. Cifra `simetrico`.
3. Intenta abrir `simetrico` ¿Puedes leer el texto?
4. Intenta abrir `simetrico.gpg` ¿Puedes leer el texto? ¿Quién ha creado este fichero con extensión `gpg`?
5. Descifra `simetrico.gpg`
6. Explica cómo y cuándo has empleado la contraseña de cifrado/descifrado.

Cifrado asimétrico

Usa el comando gpg (de GnuPG) para cifrar y descifrar de forma asimétrica

1. Genera un par de claves (privada y pública)
2. Lista las claves públicas y privadas que hay en tu anillo de claves.
3. Exporta la clave pública a un archivo en formato ASCII y nombrarlo `tunombre.pub`.
4. Realiza una copia de seguridad de la clave privada y guárdala como `tunombre.priv` (debe mantenerse segura y no compartirse).
5. Sube tu clave pública al foro de Aules (`tunombre.pub`).
6. Descarga la clave pública de un compañero, importarla y verifica que la importación es correcta.
7. Crea un archivo con algún texto y cifrarlo para el compañero, nombrándolo `PARAcompaneroDEtunombre`.
8. Sube el fichero cifrado al foro de Aules.
9. Descarga los mensajes recibidos de compañeros y descifrarlos.
10. Almacena tu clave pública en un servidor de claves.

11. Sospechas que tu clave privada ha sido comprometida, revócala:
    a. Crea un certificado de revocación.
    b. Importa el certificado de revocación que has generado.
    c. Lista primero tu anillo de claves públicas y luego el de claves privadas, y comprueba qué clave ha sido revocada.
    d. Una clave pública revocada no puede utilizarse para cifrar mensajes, aunque sí puede emplearse para descifrar aquellos que se hayan generado antes de la fecha de revocación ¿Qué ocurrirá si intentas cifrar un archivo con una clave pública revocada?

Funciones hash

1. Calcula las sumas MD5 (`md5sum` en Linux) de dos documentos y compara los valores obtenidos.
2. Analiza la diferencia en los valores hash de documentos que solo difieren en una letra.

Firma digital

Usa el comando gpg (de GnuPG) para generar y verificar una firma digital

1. Crea un archivo de prueba `documento`.
2. Genera un nuevo par de claves asimétricas.
3. Firma `documento` y llama al resultado `firmado`.
4. Verifica `firmado`.
5. Verifica `firmado` y extrae su contenido.
6. ¿Cuándo deberíamos usar el parámetro `--clearsign`? ¿Cómo se emplea?
7. ¿Qué ocurre si ejecutamos el siguiente comando `gpg --detach-sign -a documento`? ¿Cuándo crees que se debe usar?
8. Verifica el fichero `documento.asc`.

Crea tu certificado digital

Crea un certificado autofirmado con OpenSSL y consérvalo en un lugar seguro, lo utilizaremos en otras unidades.

Certificados digitales web

Examina el certificado digital utilizado por cualquier sitio web seguro (*https*) y responde a las siguientes preguntas.

1. ¿Dónde podemos encontrar…?

i. la clave pública almacenada?
ii. la firma digital de la autoridad de certificación (CA)?
iii. el periodo de validez del certificado digital?
iv. un hash del certificado?

Análisis del protocolo de cifrado de WhatsApp

- WhatsApp usa criptografía híbrida combinando el protocolo de curva elíptica Diffie-Hellman y AES.
- Uso de HMAC-SHA256 para garantizar integridad y autenticidad de los mensajes.
- Implementación de secreto hacia adelante con rotación de claves.

Firma de documentos antes de subirlos a Aules usando OpenSSL

Criterios de evaluación

- Uso de sistemas de identificación como firmas electrónicas y certificados digitales.
- Evaluación mediante cuestionario y documento de respuestas.

Herramientas de evaluación

- **Cuestionario (70%)**: preguntas de completar, verdadero/falso, opción múltiple.
- **Documento de respuestas (30%)**: respuestas del estudiante entregadas en formato de texto.