Encriptación y desencriptación con algoritmos asimétricos

Oriol Creus, Dhayan Escobar y Joel Aguilera

Índice

1. ¿En qué consiste nuestro proyecto?
2. ¿Qué aplicación real podría tener?
3. Explicación de los scripts
4. Demostración

1. ¿En qué consiste nuestro proyecto?

Realización de 2 scripts:

Script 1:

- Coge un fichero de texto (**.txt**) con un mensaje.
- Lo **encripta** con la clave **pública** del **receptor**.
- Lo **firma** con la clave **privada** del **emisor**.
- Lo guarda con fecha y hora del día, listo para enviar.

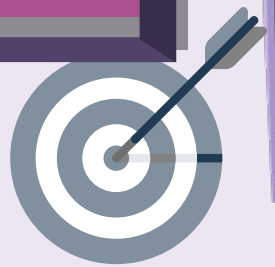
1. ¿En qué consiste nuestro proyecto?

Realización de 2 scripts:

Script 2:

- Coge el **mensaje encriptado** y comprueba que la clave con la que viene firmada coincide con la **clave pública** de quien esperamos recibir el mensaje.
- Lo **desencripta** con la **clave privada** del **receptor**.
- Lo guarda en un fichero de texto (.txt) con la fecha y hora que corresponda.

2. ¿ Qué aplicación real podría tener?



Comunicaciones seguras entre dos entidades/personas que intercambien información regularmente

Creación de claves

Clave 1 emisor privada:
openssl genpkey -algorithm RSA -aes-256-cbc -pkeyopt rsa_keygen_bits:4096 -out /home/alumne/Escriptori/script/emisor_privada.pem

Clave 2 emisor pública:
openssl pkey -in /home/alumne/Escriptori/script/emisor_privada.pem -pubout -out /home/alumne/Escriptori/script/emisor_publica.pem

Clave 3 receptor privada:
openssl genpkey -algorithm RSA -aes-256-cbc -pkeyopt rsa_keygen_bits:4096 -out /home/alumne/Escriptori/script/receptor_privada.pem

Clave 4 receptor pública:
openssl pkey -in /home/alumne/Escriptori/script/receptor_privada.pem -pubout -out /home/alumne/Escriptori/script/receptor_publica.pem


3.
Explicación de los scripts

SCRIPT 1

```
#!/bin/bash

echo "Introduce la ruta completa del archivo que deseas encriptar (por ejemplo:
/home/isard/archivo.txt):"
read ruta_archivo

if [ ! -f "$ruta_archivo" ]; then
        echo "El archivo no existe. Por favor, asegúrate de que la ruta es correcta."
        exit 1
fi

echo "Introduce la ruta completa donde quieras guardar los archivos encriptados y firmados (por
ejemplo: /home/isard/mensajes_enviar/):"
read ruta_destino

if [ ! -d "$ruta_destino" ]; then
        echo "La carpeta de destino no existe, creando la carpeta..."
        mkdir -p "$ruta_destino"
fi

fecha=$(date +"%Y-%m-%d_%H-%M-%S")

openssl pkeyutl -encrypt -inkey receptor_publica.pem -pubin -in "$ruta_archivo" -out
"$ruta_destino/$fecha.txt.enc"

openssl dgst -sha256 -sign emisor_privada.pem -out "$ruta_destino/$fecha.txt.sig"
"$ruta_destino/$fecha.txt.enc"

echo "El archivo ha sido cifrado y firmado correctamente. Puedes encontrarlo en: $ruta_destino"
```

SCRIPT 2

```
#!/bin/bash

echo "Introduce la ruta completa del archivo cifrado que quieres desencriptar (por ejemplo:
/home/isard/mensajes_enviar/2025-11-12_12-30-45.txt.enc):"
read ruta_archivo_cifrado

if [ ! -f "$ruta_archivo_cifrado" ]; then
   echo "El archivo cifrado no existe. Por favor, asegúrate de que la ruta es correcta."
   exit 1
fi

echo "Introduce la ruta completa donde deseas guardar el archivo descifrado (por ejemplo:
/home/isard/mensajes_recibidos/):"
read ruta_destino

echo "Introduce la ruta completa del archivo de la firma (por ejemplo:
/home/isard/mensajes_enviar/2025-11-12_12-30-45.txt.sig):"
read ruta_firma

if [ ! -f "$ruta_firma" ]; then
   echo "El archivo de firma no existe. Por favor, asegúrate de que la ruta es correcta."
   exit 1
fi
```

SCRIPT 2

```
echo "Comprobando la firma con la clave pública del emisor..."
openssl dgst -sha256 -verify emisor_publica.pem -signature "$ruta_firma"
"$ruta_archivo_cifrado"
if [ $? -ne 0 ]; then
   echo "La firma no es válida."
   exit 1
fi

echo "Desencriptando el archivo con la clave privada del receptor..."
openssl pkeyutl -decrypt -inkey receptor_privada.pem -in "$ruta_archivo_cifrado" -out
"$ruta_destino/$(basename "$ruta_archivo_cifrado" .enc).descifrado.txt"

if [ $? -eq 0 ]; then
   echo "El archivo ha sido desencriptado correctamente y guardado en: $ruta_destino"
else
   echo "Ha habido un error al desencriptar el archivo."
   exit 1
fi
```

4. Demostración

VAMOS A VERLO EN VIVO Y EN DIRECTO...

¡GRACIAS POR VUESTRA ATENCIÓN!