Práctica: confidencialidad con clave pública en OpenSSL

Seguridad de Sistemas Informáticos

Tercera Práctica

Resumen

El objetivo de está práctica es trabajar con esquemas de cifrado asimétrico disponibles en OpenSSL.

1. Generación de claves

1. Tenemos que generar tres claves privadas RSA de diferentes tamaños. Anota en un pequeño informe cuál es la salida que obtienes en consola, el tiempo que tarda (puedes usar el comando time de Linux) y el valor de la clave pública e.

   - Genera una clave de 2.048 bits y almacénala en un fichero.
   - Genera una segunda clave de 4.096 bits indicando que la clave pública e es la estándar y almacénala en un fichero distinto.
   - Genera otra clave de 1.024 bits indicando que la clave pública e es igual a 3.
   - Convierte las claves generadas a formato texto (hexadecimal) con el comando:

   ¿Qué conclusiones puedes extraer?

2. Almacenando las claves y generando claves públicas

1. Cifra una de las claves privadas anteriores con el triple DES.
2. Convierte una de las claves anteriores del formato PEM al formato DER.
3. Muestra las componentes de una clave privada en la consola.
4. Obtén la clave pública asociada a una de las claves privadas que generaste en el ejercicio anterior y almacénala en el fichero pubkey.pem.

3. Cifrando

1. Usando la clave pública RSA que obtuviste en el ejercicio anterior (almacenada en pubkey.pem), cifra el fichero DancingMan.txt almacenando el resultado en el fichero cipher.txt en formato hexadecimal. Genera

también el fichero resultante en binario porque para descifrarlo posteriormente lo necesitarás con esa codificación.

2. Usando la clave privada correspondiente a la pública generada anteriormente descifra el contenido del fichero cipher.txt y almacena el resultado en el fichero plain.txt. Para poder hacerlo el fichero con el texto cifrado debe estar codificado en binario, no en hexadecimal.

3. Usando la clave privada anterior firma el fichero plain.txt, almacenando el resultado en signature.bin.

4. Usando la clave pública del fichero pubkey.pem, y la firma generada en el ejercicio anterior, verifícala obteniendo el texto original en el fichero contenido.txt