Práctica 3: Autenticación de mensajes

1. Preparación del certificado

1.1 Crear una clave pública y una privada con OpenSSL

Lo primero que deberemos de hacer es crear una clave pública y una privada para nuestro uso. Para ello las crearemos en un solo archivo haciendo uso del comando:

$ sudo openssl genrsa -out certificado.pem 2048

A continuación podemos utilizar el comando **rsa** para extraer en otro fichero .pem sólo la clave pública y sólo la clave privada.

openssl rsa -in certificado.pem -out clave_publica.pem -pubout
openssl rsa -in certificado.pem -out clave_privada.pem

2. Conceptos básicos de cifrado asimétrico

Crear un texto corto (una línea) en un archivo de texto

2.1 Para cifrar con la clave pública:

openssl rsautl -in texto.txt -out texto.rsa -inkey clave_publica.pem -pubin -encrypt

- ¿qué significa cada opción?
- ¿Pide el password?
- ¿Cuál es la longitud máxima de fichero que se puede cifrar por este método?

2.2 Para descifrar con la clave privada:

openssl rsautl -in texto.rsa -out texto_recuperado.txt -inkey clave_privada.pem -decrypt
openssl rsautl -in texto.rsa -out texto_recuperado.txt -inkey certificado.pem -decrypt

- ¿qué significa cada opción?
- ¿Pide el password?

3. Envío de un mensaje cifrado a un compañero

Para cifrar ficheros grandes se suelen combinar algoritmos simétricos con asimétricos. Realizar con openssl los siguientes pasos para poder enviar por correo electrónico un archivo grande.

- Preparar un fichero grande, por ejemplo una foto.
- Cifrar el fichero utilizando un algoritmo simétrico.
- Por correo electrónico, intercambiar con un compañero las claves públicas.
- Cifrar con RSA la clave utiliza para el cifrado simétrico.
    - La clave utilizada para el cifrado simétrico debe guardarse en un fichero de texto para poder cifrarla con RSA
    - ¿qué clave habrá que utilizar para cifrar con RSA?
    - Al realizar este cifrado RSA, openssl no debe pedir ninguna clave.
- Enviar al compañero el archivo cifrado (simétrico) junto con la clave cifrada (en asimétrico).
- Deshacer los cifrados para obtener el archivo original. Para obtener la clave simétrica, deberíamos utilizar nuestra clave privada.

4. Envío de un mensaje firmado

4.1 Obtener el resumen de un documento

Utilizar el comando dgst de openssl para generar el resumen del documentos

- openssl dgst –md5 fichero.doc
- openssl dgst –sha1 fichero.doc

4.2 Cifrar el resumen

Realizar los siguientes pasos:

- Guardar el código de resumen en un fichero de texto
- ¿Qué clave hay que utilizar para el cifrado RSA?
- Cifrar dicho fichero de manera asimétrica con la clave privada, mediante el comando:

    openssl rsautl -sign -in sha.txt -inkey prikey.pem -out sig.txt

4.3 Enviar por correo electrónico

Enviar a un compañero los siguientes elementos:

- Documento original, sin cifrar
- La firma electrónica (código de resumen cifrado con la clave privada: sig.txt)
- La clave pública

4.4 Verificar la firma

Realizar los siguientes pasos para verificar la integridad del documento recibido:

- Obtener el resumen del documento (mediante MD5 o SHA)
- Comparar con el resultado de extraer el resumen de sig.txt: *openssl rsautl -verify -in sig.txt -inkey pubkey.pem –pubin –raw*