Práctica 4. Uso de OpenSSL para Cifrado de Mensajes y Ficheros

Temporalización

- Semana 7 y 8.

Parte 1

Objetivos

- Usar openssl para realizar operaciones de cifrado.
- Cifrar y descifrar información usando algoritmos de clave simétrica.
- Cifrar y descifrar información usando algoritmos de clave asimétrica.
- Experimentar con el impacto sobre la naturaleza de la información que tiene el cifrado de ficheros.

Plan de Trabajo

- Presentación de la sesión (profesor).
- Cifrar y descifrar ficheros.
- Estudio y análisis de características de los ficheros cifrados/descifrados.

Tareas a realizar

1. Usa la página de manual de **`openssl`** para obtener información sobre la forma de usar esta herramienta para cifrar y descifrar ficheros.
2. Experimenta con diversos algoritmos (AES, DES, CAMELLIA,) y modos de cifrado (ECB, CFB, CBC). Utiliza diferentes ficheros de entrada (texto y binarios) y con diferentes claves y vectores de inicialización.
3. Obtenga información sobre el concepto de entropía de Shanon y elabore un breve informe y discusión sobre el tema. Usando el programa Python (enlaces interesantes), obtenga la entropía de los ficheros usados en el apartado segundo (tanto cifrados como

descifrados), así como la del fichero obtenido en el apartado cuarto y la de un fichero que contenga un único byte repetido un número de veces arbitrario.

4. Obtenga de la red un fichero que contenga una imagen en formato BMP (libre de derechos, a poder ser) y cífrelo usando AES con modos ECB y CBC. Salve copias de la imagen cifrada, sustituya por la cabecera (54 bytes) del fichero original las cabeceras de los ficheros obtenidos y cárguelos en un programa de visualización de imágenes. Comente el resultado. Nota: Para trasladar la cabecera de un fichero in.bmp a otro out.bmp dejando el resto inalterado, se puede usar: '`dd if=in.bmp of=out.bmp bs=54 count=1 conv=notrunc`'

Enlaces de interés

- https://www.openssl.org/docs/manmaster/man1/openssl-enc.html
- https://www.openssl.org/docs/manmaster/man1/enc.html
- https://www.openssl.org/docs/man1.0.2/apps/rsautl.html
- https://raymii.org/s/tutorials/Encrypt_and_decrypt_files_to_public_keys_via_the_OpenSSL_Command_Line.html
- Calculate File Entropy – Kenneth G. Hartman, CISSP (kennethghartman.com)
    - https://campusvirtual.uva.es/pluginfile.php/719368/mod_page/content/26/entropia.py
    - https://campusvirtual.uva.es/pluginfile.php/719368/mod_page/content/26/entropia_plt.py
- https://wiki.openssl.org/index.php/Main_Page
- https://publicdomainreview.org/collections/albert-racinets-lornement-polychrome-1869-73/

Temporalización

- Semana 9 y 10.

Parte 2

Objetivos

- Comprender los principios básicos de la gestión de claves y certificados.
- Ser capaz de generar claves RSA, protegidas o no.
- Ser capaz de generar solicitudes de firma de claves.
- Ser capaz de firmar y revocar certificados.
- Instalar y usar una CA usando OpenSSL.

Tareas a realizar

1. Selecciona un servidor web público (puedes utilizar el de la UVa) e investiga cuáles son los puertos a nivel de transporte que utiliza para brindar el servicio web. ¿Qué sentido tiene?
2. Analiza el certificado digital presente en el servidor web. Puedes hacer udo de la herramientas sslscan y ssltest del apartado anterior e indica:
    a. Protocolo/s criptográfico y versión utilizado a nivel de transporte.
    b. Algoritmo de criptografía asimétrica (clave pública) utilizado y longitud de la clave pública.
    c. Indica la clave pública presente en el certificado digital. ¿Por qué se utiliza esa y no otra?
    d. Algoritmo de criptografía simétrica (clave privada) utilizado y longitud de la clave privada.
    e. Algoritmo de firma digital utilizado en el certificado digital.

3. Explica con un diagrama de secuencia por qué en un certificado digital se usa criptografía de clave pública y privada.
4. Utiliza la herramienta OpenSSLpara la generación de un vertificado digital que tenga una longitus de clave de 1024 bits y analízalo con *sslscan* y *ssltest*.

Temporalización

- Semana 9 y 10.

Parte 3

Objetivos

- Entender el rol que juega el certificado en el proceso de firma digital de documentos.
- Ser capaz de firmar archivos y verificar la firma.
- Entender el funcionamiento práctico de la firma digital.

Plan de Trabajo

- Instalación de entorno PGP4WIN (gpg4win) / Kleopatra.
- Preparación de identidades e intercambio de claves.
- Envío y recepción de mensajes cifrados y/o firmados

Tareas a realizar

1. Explica el proceso de firma digital y comprobación de la validez de la firma garantizando sólo los principios de Autenticidad y de No Repudio. Realiza lo mismo para garantizando, además, el principio de Integridad de la información.
2. Cada estudiante deberá asociarse con otro estudiante con quien intercambiará claves.
3. Debe comenzar instalando el software pgp4win en su equipo (Windows) o en el de laboratorio (instalación de usuario).
4. Cree un usuario e identidad y una pareja de claves (certificado).
5. Exporte la clave pública de su certificado y comparta la misma con el compañero. Cada uno deberá haber recibido la clave de al menos otro compañero.
6. Importe la clave pública que le haya enviado su compañero/a.

7. Cree un fichero de texto o use un fichero que ya tenga (puede ser TXT, DOC, PDF, ...; ojo, porque tendrá que modificarlo luego).
8. Cifre el fichero usando Kleopatra y seleccionando el certificado recibido de su compañero/a.
9. Envíe el fichero cifrado adjunto a un correo electrónico al compañero/a seleccionado. 9. Cuando reciba el que su compañero/a le envíe a usted, proceda a descifrarlo.
10. Repita los pasos 7 al 9 pero ahora firme el fichero en lugar de cifrarlo (puede cifrarlo y firmarlo también, si quiere, pero recuerde que deberá cifrarlo con la clave pública del destinatario). Ahora deberá adjuntar el fichero original y la firma digital asociada al mismo.
11. Compruebe que el fichero y firma que le hayan enviado sean correctos y provengan de quien dice enviarlos. Modifique el fichero recibido y vuelva a comprobar la firma, analizando qué ocurre.
12. Genera un certificado difital con RSA con una longitud de clave pública de 2048 bits. Securiza el directorio que contendrá la clave privada del certificado.
13. ¿Qué ocurre si alguien es capaz de robar la clave privada utilizada por un certificado digital? Justifica tu respuesta.