Fundamentos de Seguridad – Análisis de la seguridad en los Sistemas de Información – CURSO 2019-2020

Práctica 1: Taller de OpenSSL. Cifrado (simétrico y asimétrico), resúmenes, certificados X.509, correo S/MIME, correo PGP y servidor seguro SHTTP.

PARTE 1 - Utilización de OpenSSL (cifrado simétrico, resúmenes, claves asimétricas, firma y cifrado asimétrico)

1.1 Cifrado Simétrico de documentos

Seguir los siguientes pasos para crear un documento de texto y cifrarlo con openssl (preferiblemente instalando la última versión 1.1.1):

- Estudiar en la documentación de openssl cómo se utiliza el comando enc para cifrar y descifrar. Explicar sus opciones más importantes, con especial atención a los métodos de cifrado (ecb, cbc, etc.).
- Crear un archivo de texto legible (pequeño tamaño – entre 260 y 300 caracteres)
- Cifrarlo con CINCO algoritmos simétricos (AES y TDES obligatorios y un cifrador de flujo como mínimo).
- Descifrarlos y comprobar el resultado
- Explicar el tamaño de los diferentes ficheros cifrados en virtud del tamaño de bloque del cifrador (o no, si es un cifrador de flujo), y sabiendo que el empleo de sal añade 16 bits de más al inicio del fichero cifrado –Salted__XXXXXXXX-.
- **Explicar la gestión de contraseñas** detallada en el estándar PKCS #5 (PBKDF1 y PBKDF2) y su aplicación a las claves de cifrado simétrico, vectores de inicialización y sal (derivación de claves e “iv” a partir de contraseñas). Documentar las diferentes alternativas, empleando diferentes algoritmos de cifrado. **Demostrar que un fichero puede ser cifrado con contraseña y descifrado con su conjunto equivalente de clave (key), vector de inicialización (iv) y sal (salt)**.

  Documentar el trabajo realizado, **con ejemplos de los resultados obtenidos (valores binarios en hexadecimal, Base64 o en formato PEM) y profusión de volcados de pantalla**.

  Opcional: Se valorará muy positivamente la **demostración** de que el modo de operación **“ecb” es muy peligroso**, por ejemplo, con una **imagen de colores sólidos** (similar al ejemplo de “Tux” en la página de Wikipedia) en este caso, utilizar el formato PGM y cifrar el cuerpo de la imagen sin hacerlo con la cabecera.

1.2 Generación y comprobación de Resúmenes. Generación de claves asimétricas (pública-privada) y firmado de resúmenes

- Utilizando la **bibliografía acerca de OpenSSL de la página de la asignatura**, utilizar diferentes algoritmos de resumen (TRES de los más modernos) sobre un archivo de texto y comprobar dichos resúmenes ante **mínimas** modificaciones del fichero.
- **Generar un par de claves asimétricas RSA** de 2048 bits, de acuerdo con las indicaciones del apéndice A del manual básico (para RSA).
- **Exportar dicho par de claves** (pública y privada) en formato PEM (textual) y DER (binario). Utilizar los comandos de conversión de PEM a DER y viceversa.
- Con los dos pares de claves asimétricas creadas, **firmar y comprobar la firma** del resumen (con SHA-256) de un texto cualquiera.
- Por último. Generar dos claves DH (preferiblemente con curva elíptica X25519) y demostrar que la combinación pública1-privada2 genera el mismo secreto que la combinación privada1-pública2.

  Documentar el trabajo realizado, **con ejemplos de los resultados obtenidos (en Base64 o en formato PEM) y profusión de volcados de pantalla**.

  Opcional: **Repetir** estas operaciones con claves **DSA**. Su generación exige búsqueda de documentación y el empleo de la utilidad "dsaparam".

1.3 Cifrado Asimétrico de documentos

Seguir los siguientes pasos **para crear un documento de texto y cifrarlo con openssl, enviando a un compañero el documento cifrado y la clave, cifrada a su vez con su clave pública RSA** (que previamente ha de conocerse). Codificarlo todo en Base64 y enviar un correo electrónico con tres partes:

1.- Documento cifrado (indicando algoritmo utilizado)
2.- Clave simétrica empleada, cifrada con la clave pública del receptor
3.- Resumen del documento original (indicando algoritmo) cifrado con la clave privada del emisor

El mensaje **ha de ser de tipo textual**, indicando las diferentes partes e instrucciones para su decodificación/comprobación (comandos OpenSSL necesarios para decodificar y verificar el documento).

Se valorará positivamente el empleo de diferentes sistemas de cifrado, de generación de resúmenes, etc.

Documentar el trabajo realizado, **con ejemplos de los resultados obtenidos (en Base64 o en formato PEM) y profusión de volcados de pantalla**.

Documentación del trabajo efectuado

Preparar un **DOCUMENTO DE TEXTO** (en formato RTF o mejor aún, PDF) **documentando exhaustivamente los pasos realizados en cada una de las CUATRO PARTES de esta práctica**. El número de páginas no será inferior a 15, y se incluirán listados de todos los ficheros obtenidos (textos de ejemplo, ficheros cifrados, resúmenes, firmas, etc.) en formato texto, hexadecimal, base64, PEM o similar, según cada caso. **El documento ha de estar formado por CUATRO capítulos**, correspondientes a los tres ejercicios propuestos en esta práctica, en los que se describa con detalle las operaciones realizadas.

Se aconseja incluir una **portada** con los datos del estudiante, título del trabajo (Practica 1 de la asignatura ....) un **índice** de los capítulos, una **bibliografía** con los recursos utilizados (libros, páginas web, etc.) y en general, todo aquello que estimemos debe incorporar un **trabajo de calidad profesional**.

Se valorará tanto la **calidad técnica del trabajo como la claridad de la redacción**, el empleo de fuentes específicas para distinguir el texto escrito de los comandos utilizados (se aconseja una fuente del tipo Courier de paso fijo para comandos y ficheros de texto), la **inserción de volcados de pantalla** para mostrar textos, páginas web o resultados de opciones del navegador, la ausencia de faltas ortográficas y la profesionalidad del trabajo en general. **En este sentido, será obligatorio personalizar el "prompt" del sistema operativo (PS1='apellido>'),** de forma que los volcados de pantalla sean lo más personales posible.

El documento final, de nombre ***PRACTICA1.PDF*** o ***PRACTICA1.RTF***, será entregado en el contenedor denominado ***ENTREGA DE LA PRÁCTICA 1***, en la página principal de la asignatura, en el Campus Virtual de la ULPGC.

Será **CONDICIÓN IMPRESCINDIBLE para aprobar** esta práctica el obtener como mínimo **CINCO puntos sobre 10 en cada una de las cuatro partes**, por tanto, no se podrá superar la práctica sin haber realizado buena parte de lo que se solicita en cada una de sus partes.

Recordemos que ES IMPRESCINDIBLE la REVISIÓN Y DEFENSA DEL TRABAJO en ENTREVISTA PERSONAL con el profesor. A finales del curso se establecerán las fechas para realizar estas entrevistas en la que cada estudiante muestre y defienda todas sus prácticas **y sean calificadas por el profesor**.