Ejercicios de la UD06

1. Training

1. **Ejercicio 1: Comprobación de integridad.**

   Programa una aplicación que reciba como parámetros de entrada un fichero y su HASH SHA-512 y que certifique la integridad del fichero. Puedes obtener ficheros y HASH de pruebas en la sección de descargas de Hak5: https://downloads.hak5.org/

2. **Ejercicio 2: Hashes salados**

   Investiga que son los Hashes salados y porqué es necesario añadir "sal" a nuestros hashes. Investiga y explica como guarda el hash salado el el sistema operativo GNU/Linux en el archivo `/etc/shadow`. Modifica el **`Ejemplo2`** de manera que incorpore "sal" a los hashes. Debe añadir sal al registrar una credencial y tenerla en cuenta al validar el password.

3. **Ejercicio 3: Almacenamiento seguro.**
   Programa una aplicación Java que reciba como parámetros de entrada un fichero y una contraseña, cifre el contenido utilizando AES, almacene el resultado con un nombre de fichero distinto y borre el fichero original. Programar también la aplicación que realice la transformación inversa.

4. **Ejercicio 4: Confidencialidad e identidad.**

   Programa una aplicación Java que, dado un fichero, lo cifre primeramente con la clave privada del emisor y, posteriormente, con la clave pública del destinatario. Programa también la aplicación que descifre el fichero.

5. **Ejercicio 5: Firmado digital de documentos.**
   Diseña y desarrolla un sistema en Java que solicite un fichero y genere la firma digital del mismo. Crea el programa capaz de validar que el documento firmado no ha sufrido alteraciones y que el emisor es quien dice ser.

6. **Ejercicio 6: Socket seguro**

   Realizando parejas o tríos, preparad el entorno del **`Ejemplo6`**, de modo que un alumno realice las tareas de servidor, y otro u otros de cliente (no simultáneos). Generad todas las claves/certificados/almacenes necesarios y cuando el sistema esté funcionando enseñadlo al profesor para su evaluación.

2. Questions

1. ¿Cómo se llama al par identificador-contraseña de un sistema de seguridad?
   a) Perfil.
   b) Credencial.
   e) Autorización.
   d) Rol.
2. ¿Cuál de las siguientes características físicas no puede ser un control de acceso biométrico?
   a) La voz.
   b) La huella dactilar.
   c) El reconocimiento facial.
   d) La altura.
3. ¿Por qué se deben almacenar los resúmenes de las contraseñas en lugar de estas?
   a) Para ahorrar espacio.
   b) Para impedir obtener la contraseña.
   c) Para validar más rápidamente las credenciales.
   d) Para evitar que dos usuarios tengan la misma contraseña.
4. ¿Qué parte de un sistema criptográfico debe ser secreto?
   a) El algoritmo utilizado para cifrar.
   b) La longitud de las contraseñas.
   c) Las contraseñas.
   d) Los identificadores de usuario.
5. ¿Cuál de las siguientes características no es propia de un sistema criptográfico de clave simétrica?
   a) Es reversible.
   b) La salida generada por el algoritmo tiene un tamaño constante.
   c) No puede tener pérdidas de información.
   d) La clave es única y válida tanto para cifrar como para descifrar.
6. ¿Cuál de los siguientes algoritmos no es un algoritmo HASH?
   a) MD5.
   b) SHA-2.
   e) SHA-3.
   d) DES.
7. ¿Cuál de los siguientes algoritmos es un algoritmo de clave pública?
   a) AES.
   b) RC5.
   c) Blowfish.
   d) RSA.
8. ¿Cuál de los siguientes algoritmos se utiliza para realizar la firma digital?
   a) RSA.
   b) DSA.
   e) AES.
   d) SHA-2.
9. ¿Cuál de los siguientes algoritmos se utiliza para almacenar información cifrada?
   a) Blowfish.
   b) AES.
   e) RSA.
   d) DES.

10. ¿Qué se garantiza con la firma digital?
    a) La integridad del mensaje.
    b) La identidad del receptor.
    c) La confidencialidad.
    d) La seguridad del canal de comunicación.
11. ¿Cuál es el punto débil de utilizar un algoritmo de clave simtrica en transferencia de datos?
    a) El canal.
    b) La distribución de las contraseñas.
    c) La seguridad intrínseca del algoritmo.
    d) La existencia de colisiones.

3. Actividades de aplicación

1. Algunos algoritmos criptográficos con el paso del tiempo han dejado de ser seguros. Indica las razones principales.
2. Define en qué consiste el control de acceso basado en credenciales.
3. Describe el proceso de almacenamiento de credenciales utilizando resúmenes (HASH).
4. Explica el procedimiento de verificación de credenciales utilizando resúmenes (HASH).
5. Indica por qué hay que utilizar resúmenes (HASH) para almacenar contraseñas en lugar de utilizar algoritmos simétricos.
6. Explica cómo se puede utilizar un algoritmo HASH para garantizar la integridad de un mensaje.
7. Los algoritmos de HASH pueden tener colisiones. Explica qué son y por qué se acepta como válido que exista la remota posibilidad de que se produzcan.
8. Explica en qué consiste la firma digital de un documento.
9. Describe el riesgo inherente a utilizar protocolos no seguros (sockets TCP o HTTP) en la transferencia de información.
10. Explica por qué es conveniente cambiar las contraseñas cada cierto tiempo.
11. Haz una exposición sobre las razones para evitar utilizar sitios web que sean capaces de mostrar las contraseñas en claro.
12. Explica el proceso mediante el cual se puede garantizar la identidad del emisor y la confidencialidad de un mensaje utilizando un algoritmo de clave pública.
13. Encuentra al menos tres recomendaciones sobre cómo crear una contraseña segura y elabora tu propia recomendación.

4. Actividades de ampliación

1. Profundiza en el conocimiento del cifrado César. Averigua cómo descifrar un texto cifrado con este sistema.
2. Explica que implicación tienen los algoritmos de clave simétrica y asimétrica en las conexiones VPN. ¿Se usan los dos? ¿solo uno? ¿cuál es mejor? Explica como se establece la conexión y la posterior comunicación de manera segura.
3. Busca sitios web que generen HASH. Comprueba que los resúmenes que generan todos ellos son los mismos dadas las mismas entradas.
4. Descubre en qué se diferencian los cifrados de flujo de los cifrados de bloque.
5. Investiga sobre el uso de la firma digital. Descubre para qué se puede utilizar en la Administración Pública y qué herramientas online existen para verificar que un documento está firmado correctamente.
6. Averigua en qué se diferencian las versiones del algoritmo AES siguientes: AES-CBC, AES-CFB, AES-OFB.
7. Estudia cómo funciona el protocolo HTTPS.
8. Descubre qué funcionalidad proporciona el servicio Java Authentication and Authorization Service (JAAS).
9. Averigua qué utilidad tiene la extensión de Java Secure Socket Extension (JSSE).

5. Fuentes de información

- Wikipedia
- Programación de servicios y procesos - FERNANDO PANIAGUA MARTÍN [Paraninfo]
- Programación de Servicios y Procesos - ALBERTO SÁNCHEZ CAMPOS [Ra-ma]
- Programación de Servicios y Procesos - Mª JESÚS RAMOS MARTÍN - [Garceta] (1ª y 2ª Edición)
- Programación de servicios y procesos - CARLOS ALBERTO CORTIJO BON [Sintesis]
- Programació de serveis i processos - JOAR ARNEDO MORENO, JOSEP CAÑELLAS BORNAS i JOSÉ ANTONIO LEO MEGÍAS [IOC]
- GitHub repositories:
    - https://github.com/ajcpro/psp
    - https://oscarmaestre.github.io/servicios/index.html
    - https://github.com/juanro49/DAM/tree/master/DAM2/PSP
    - https://github.com/pablohs1986/dam_psp2021
    - https://github.com/Perju/DAM
    - https://github.com/eldiegoch/DAM
    - https://github.com/eldiegoch/2dam-psp-public
    - https://github.com/franlu/DAM-PSP
    - https://github.com/ProgProcesosYServicios
    - https://github.com/joseluisgs
    - https://github.com/oscarnovillo/dam2_2122
    - https://github.com/PacoPortillo/DAM_PSP_Tarea02_La-Cena-de-los-Filosofos