Seguridad de la Información – CURSO 2025-2026

Práctica 2: Algoritmos de resumen y de cifrado simétrico

Los objetivos de esta práctica son el manejo de comandos de la herramienta OpenSSL para la realización de operaciones criptográficas de uso de algoritmos de **resumen** y de **cifrado simétrico**.

Previo a la realización de la práctica, es imprescindible:

- Tener instalado OpenSSL versión 3 o superior
- Asegurarnos de que tenemos activado el Provider Legacy (compatibilidad con algoritmos antiguos u obsoletos).
- Conocer el manejo básico de OpenSSL en modo comando, especialmente:
  - openssl-dgst
    - Algoritmos de resumen (-md5 -sha1 -sha-256 -whirlpool, etc.)
  - openssl-enc
    - Algoritmos, modos de operación (openssl enc -list-ciphers)
    - Ficheros cifrados binarios y en BASE64
    - Cifrado con contraseña (y sal) o con clave/vector
    - Derivación de claves a partir de contraseña: -pbkdf1 y -pbkdf2 (**pbkdf2** será siempre **obligatorio**)
  - Otros comandos

Documentación básica:

- Documentación de Openssl (https://www.openssl.org/docs/man3.2/index.html)
- Openssl Howto (https://openssl.cicei.com)
- Estándares PKCS (https://es.wikipedia.org/wiki/PKCS)1,3,5,7,8,10,12
  - PKCS #5: Derivación de contraseña PBKDF1 y PBKDF2
    - https://en.wikipedia.org/wiki/PBKDF2
    - **Usar SIEMPRE -pbkdf2** y comprender significado de -iter (10000 por defecto) y -md (sha-256 por defecto)
- Algoritmos de resumen MD5, SHA-1, SHA2 (256,384,512), SHA-3 (idem), Whirlpool, etc.
  - Wikipedia MD5 SHA1 SHA2 etc.
- Algoritmos de cifrado simétrico AES (128, 192, 256), DES, TDES, IDEA, CHACHA20, etc.
  - Wikipedia AES DES TDES IDEA CHACHA20 etc.
- Modos de operación de cifrado en bloque:
  - (https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation)
- Formato gráfico NetPBM https://en.wikipedia.org/wiki/Netpbm
- ChatGPT (https://openai.com/chat) , DeepSeek (https://chat.deepseek.com), etc.

Práctica 2: Algoritmos de resumen y de cifrado simétrico

PREVIO: Verificación de que está activado el "Provider Legacy" en OpenSSL V3+

La versión 3 y siguientes de OpenSSL separan los algoritmos declarados obsoletos (cifrador rc4, algoritmo de resumen whirlpool, etc.) en una librería (provider) denominada "legacy". Por defecto, el uso de este proveedor está desactivado en muchas distribuciones.

Si el comando # openssl list -providers NO muestra como activo el proveedor Legacy con status "active", se debe editar el fichero de configuración (/etc/pki/tls/openssl.cnf en Fedora y similares, usualmente /etc/ssl/openssl.cnf en Kali) y asegurarnos de que la sección [provider_sect] tiene incluido el proveedor Legacy y asegurarnos de que la sección [legacy_sect] tiene activate = 1. Editado el fichero, repetir el comando openssl list -providers y comprobar que aparece Legacy como activo. En caso de duda, consultar la IA y atender especialmente a cuál de los posibles ficheros de configuración, si hubiese más de uno en directorios del sistema, está activo.

2.1 Generación y comprobación de Resúmenes

Una vez entendido el empleo del comando openssl-dgst y sus opciones básicas (-help, -list):

1. Crear un archivo de texto legible de entre 150 y 200 caracteres
2. Aplicar un mínimo de CINCO algoritmos de resumen distintos (md5, SHA-1, SHA-2 y Whirlpool son obligatorios) sobre ese archivo de texto, verificar que el tamaño coincide con la descripción del algoritmo de resumen empleado y comprobar cómo varían los resúmenes obtenidos con el mismo algoritmo ante **mínimas** modificaciones del fichero (cambiando un solo carácter, por ejemplo).
3. Alternar entre salida hexadecimal, hexadecimal con : y binaria

2.2 Cifrado Simétrico de documentos

Una vez entendido el empleo del comando openssl-enc para cifrar y descifrar, sus opciones básicas (-help y -list) con diferentes algoritmos y modos de operación, el empleo de ficheros binarios y BASE64, la derivación de claves a partir de contraseñas y sal, detallada en el estándar PKCS #5 (PBKDF1 y PBKDF2) y su aplicación a las claves de cifrado simétrico y vectores de inicialización:

1. Crear un archivo de texto legible de pequeño tamaño – entre 31 y 81 caracteres (número impar).
2. Cifrarlo (con salida en **modo binario**) con **SIETE** algoritmos simétricos (AES y TDES obligatorios, en modo bloque y flujo y dos cifradores de flujo -**rc4** y –**chacha20** o similar-).
3. Descifrarlos y comprobar el resultado
4. Explicar el tamaño de los diferentes ficheros cifrados en virtud del tamaño de bloque del cifrador (o no, si se cifra en flujo), y sabiendo que el empleo de sal añade 16 bits de más al inicio del fichero cifrado –Salted__XXXXXXXX-.
5. Cifrar el archivo con aes-256-cbc y contraseña y descifrarlo NO con dicha contraseña, sino con su conjunto equivalente de clave (key) y vector de inicialización (iv). Para ello habrá que usar "-p" en el cifrado y eliminar los 16 bits iniciales del fichero cifrado que contienen la sal aleatoria utilizada por el comando de cifrado (con el comando dd bs=1 skip=16 if= of= o similar) antes de descifrarlo con -k y -iv, poniendo sus valores mostrados al cifrarlo por la opción "-p".

2.3 Aplicación: Demostración de la peligrosidad del modo de operación ECB

En este apartado demostraremos que el modo de operación "ecb" con cifradores simétricos es muy peligroso, repitiendo el ejemplo de Wikipedia con el pingüino Tux, utilizando una imagen pequeña con colores sólidos como entrada. Para ello:

1. Escogeremos una imagen de entre **20 y 50** Kb de colores sólidos (gif, png, etc.)
2. Con la utilidad "convert" del paquete ImageMagick o similar la convertiremos a formato PGM (ver https://en.wikipedia.org/wiki/Netpbm)
3. Separaremos la cabecera (3 primeras líneas de texto) y el cuerpo (binario) de la imagen
4. Cifraremos el cuerpo con el cifrador de bloques más potente en la actualidad (AES-256) **en modo ECB** y una clave o contraseña aleatorias, si se usa contraseña, realizar el cifrado sin sal (**-nosalt**).
5. Crearemos la nueva imagen con la cabecera anterior y el cuerpo cifrado
6. Convertiremos la nueva imagen al formato original con Imagemagick "convert"
7. Verificaremos que la nueva imagen puede ser "vista" de la misma forma que Tux en el ejemplo de Wikipedia (https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation).
8. Realizar la operación **con otro cifrador de 64 bits de bloque** (des, des-ede3, etc) en modo ECB y comparar los resultados. El menor tamaño de bloque debería acentuar las diferencias en los cambios de color en la imagen original.

Es **MUY IMPORTANTE** entender que esta parte de la práctica exige el uso de una imagen en colores sólidos (gif, png-8, etc.) que no use ningún sistema de compresión de la imagen (jpeg, jfif, etc.). Si la imagen procesada sólo muestra "ruido" usualmente se debe a que la imagen tenía algún sistema de compresión de datos y se debe utilizar otra imagen asegurándose de que utiliza colores sólidos.

Documentación y entrega de la práctica 2:

Se ha de preparar un **DOCUMENTO DE TEXTO** (en PDF) de carácter profesional, en el que **se desarrollen exhaustivamente los pasos realizados en cada una de las partes de esta práctica**. Estará precedido por una **portada** con el título de la práctica, un **índice** con los apartados que se desarrollan y el **nombre** del estudiante. El número de páginas no será inferior a 6, y se incluirán debajo del enunciado de cada apartado los comandos utilizados y los listados de todos los ficheros obtenidos en formato texto, hexadecimal, base64, PEM o similar, según cada caso. con ejemplos de los resultados obtenidos (con la parte binaria en hexadecimal, base64 o PEM) y profusión de **recortes de volcados de pantalla** en los que se ha **personalizado** el "prompt" de la consola con el nombre y apellido del estudiante (por ejemplo, en mi caso, usaría el comando **export PS1="Antonio Ocon> "). Este "prompt" personalizado se ha de mostrar en TODAS las restantes prácticas** que conlleven capturas de pantalla del sistema operativo. El documento finalizará con un apartado denominado **Bibliografía** en el que se indiquen las **referencias** más importantes en la redacción del documento (pueden ser las indicadas al comienzo de esta práctica junto a las aportadas por el estudiante). El formato de esta bibliografía debe seguir las normas IEEE (se pueden consultar en https://biblioguias.uma.es/citasybibliografia/IEEE).

Los estudiantes que **siguen la asignatura por curso defenderán personalmente cada práctica al profesor en el laboratorio**. Como máximo podrán entregar cada práctica dos semanas después del período de finalización de la misma y no se podrán defender más de dos prácticas a la vez.

Los estudiantes que **no siguen la asignatura por curso deberán subir el programa completo de prácticas a la plataforma en convocatoria extraordinaria o especial**, en las fechas indicadas en la página de la asignatura, próximas a la celebración de dichas convocatorias.