23 de octubre de 2017

Orquidea Seijas

Grado en ingeniería Informática

Escola Técnica Superior de Enxeñería

Actividad 5: Informe sobre cifrado simétrico y funciones hash

Seguridad informática

Contenido

[Título 1 1](#_Toc495918573)

# Cifrado simétrico básico.

**Incluid en el informe las respuestas a todas las cuestiones, así como todas las instrucciones y comandos utilizados, y las incidencias que hayáis encontrado durante la sesión.**

Para iniciar la sesión, se ha realizado un ejercicio para observar la diferencia entre cifrado y codificación. En primer lugar, se ha elegido una palabra como clave, de forma arbitraria, para cifrar un documento. Esta clave se ha cifrado en base64 utilizando el siguiente comando:

openssl enc -base64 -in file.txt -out filecoded.txt

Donde *file.txt* es el archivo que contiene la clave, en este caso *holi*, y *filecoded.txt* contiene la clave codificada en base64. Para comprobar que la codificación era correcta, se ha utilizado el mismo comando con la opción de decodificar:

openssl enc -base64 -d -in filecoded.txt -out filedecoded.txt

Se obtuvo la misma clave introducida al principio, por lo que se pudo concluir que la codificación había sido exitosa. A continuación, se ha utilizado la palabra escogida para cifrar un documento utilizando DES en modo CBC utilizando el comando:

openssl enc -des-cbc -in file.txt -out fileencrypted.txt

Donde *file.txt* es el fichero que contiene el texto a encriptar y *fileencrypted.txt* es el fichero que contiende el texto obtenido una vez se realiza la encriptación. Puesto que este archivo iba a ser reenviado a un compañero, se consideró necesario comprobar que la encriptación había sido exitosa y se decidió desencriptarlo:

openssl enc -base64 -d -in fileencrypted.txt -out filedecrypted.txt

A continuación, se recibieron dos ficheros por parte de un compañero: uno contenía la clave codificada

**Base64** es un esquema de codificación (**no de cifrado**) que utiliza 65 caracteres imprimibles (26 letras minúsculas, 26 letras mayúsculas, 10 dígitos, caracteres '+' y '/', el caracter especial '='). Base64 permite representar e intercambiar datos con problemas de codificación.

**Sintaxis:**Para codificar en base64, se utiliza el comando ***enc*** con la opción***-base64*** : 

*openssl enc -base64 -in*input-file *-out*output-file. 

Para decodificar, añadimos la opción ***-d***: 

*openssl enc -base64**-d -in*input-file *-out*output-file

**Ejercicio:**Elegid una **palabra o frase clave** arbitraria y guardadla en un fichero. Codificarla en base64, y enviadla a vuestro compañero. Utilizar la clave elegida para cifrar un documento usando DES en modo CBC (cambiamos la opción *-base64* por ***-des-cbc***, con lo que el comando *enc* cifra en lugar de codificar, para lo cual pedirá una clave)*.* A continuación enviar el fichero cifrado al compañero. Cada uno debe descifrar el fichero cifrado recibido, utilizando para ello la clave correspondiente (después de descodificarla).

¿Cuál es la diferencia entre cifrado y codificación?

## Diferencia entre cifrado y codificación

# Cifrado/Descifrado

* Usad el algoritmo DES en modo CBC para cifrar un texto pequeño, y a continuación, un texto más grande. Comprobad el valor del vector de inicialización en cada caso (añadiendo la opción -p al cifrar). ¿Hay alguna diferencia? ¿Para qué se utiliza este vector de inicialización IV? Verificad qué sucede si utilizamos el modo ECB.
* Comparad los resultados del cifrado usando diferentes algoritmos simétricos (des, 3des, aes con distinto tamaño de clave, ...) para cifrar los mismos ficheros, e indicad la longitud de la clave empleada en cada caso, el tamaño del bloque, el tamaño del fichero cifrado, y los vectores de inicialización si se utilizan.
* Aplicad un algoritmo de cifrado simétrico a un fichero más complejo (una imagen, un fichero pdf, ...). Comprobad que el fichero cifrado no puede abrirse con la aplicación original.
* Averiguad y explicad para qué y cómo se utiliza el rellenado ("*padding*") en los algoritmos de cifrado simétrico.

# Extracto o resumen digital

* Obtened el resumen o extracto digital (hash) de un documento de texto plano usando el algoritmo MD5 y el algoritmo SHA-1. Para calcular extractos, tenemos el comando *dgst.*¿Qué longitud tienen los resúmenes en bits en cada caso?
* Modificad un único carácter en el texto y obtened los resúmenes de nuevo. Comprobad qué sucede con el extracto (longitud, contenido). Explicad los distintos usos que puede tener un extracto digital.
* Obtened el resumen de un texto plano más grande, y de una imagen, usando el algoritmo SHA-1. Comparad las longitudes de los extractos.
* Obtened el extracto digital de los mismos ficheros empleados en los puntos anteriores, pero ahora utilizando los algoritmos SHA-256 y SHA-512. ¿Cuáles son las diferencias?

# Cifrado simétrico en HTTPS

Comprobad qué algoritmo de **cifrado simétrico** se usa para cifrar la conexión en el Campus Virtual. ¿Cuál se usa en el servidor de correo web de la USC? ¿Y en Gmail? Comprobad otros sitios web como Paypal, bancos, tiendas virtuales,... y si es posible, utilizando diferentes navegadores.

Averiguad y explicad cómo se selecciona el algoritmo simétrico a utilizar en una conexión particular.

# Referencias