23 DE OCTUBRE DE 2017

ACTIVIDAD 5: INFORME SOBRE CIFRADO SIMÉTRICO Y FUNCIONES HASH

SEGURIDAD INFORMÁTICA

ORQUIDEA SEIJAS
GRADO EN INGENIERÍA INFORMÁTICA
Escola Técnica Superior de Enxeñería

CONTENIDO

I. 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 -des-cbc -d -in fileencrypted.txt -out filedecrypted.txt
```

A continuación, se recibieron dos ficheros por parte de un compañero: uno contenía la clave codificada y otro contenía el texto cifrado. Se utilizaron los mismos comandos comentados anteriormente para la descodificación de la clave, que es *pizza*, y para la desencriptación del texto, que es el siguiente:

El lobo (Canis lupus) es una especie de mamífero placentario del orden de los carnívoros. El perro doméstico (Canis lupus familiaris) se considera miembro de la misma especie según distintos indicios, la secuencia del ADN y otros estudios genéticos. Los lobos fueron antaño abundantes y se distribuían por Norteamérica, Eurasia y el Oriente Medio. Actualmente, por una serie de razones relacionadas con el hombre, incluyendo el muy extendido hábito de la caza, los lobos habitan únicamente en una muy limitada porción del que antes fue su territorio.

a. DIFERENCIA ENTRE CIFRADO Y CODIFICACIÓN

La diferencia más significativa entre codificación y cifrado es que la transformación aplicada al elemento que se desea proteger:

Si se codifica un texto, simplemente se está realizando un intercambio, más o menos complejo, de un carácter por otro. El resultado de la codificación tiene una equivalencia directa, carácter a carácter, con el texto original, gracias a una serie de normas preestablecidas para alterar la semántica del mensaje.

Por otra parte, el cifrado de un texto, se realiza a través de un algoritmo que puede modificar la extensión y composición original. Solo es posible recuperar el texto cifrado a través de un algoritmo equivalente. El cifrado suele usar una clave para transformar la estructura, de forma tal, que, si un tercero interviene, no pueda acceder a la información. Este cifrado puede ser simétrico, siendo la clave igual a ambos sentidos de la comunicación, o asimétrico, donde se utiliza un sistema de clave pública y clave privada.

II. CIFRADO/DESCIFRADO

Con el fin de comprender mejor el funcionamiento del cifrado y descifrado, se utilizó el algoritmo DES (*Data Encryption Standard*) en modo CBC (*Cipher Block Chaining Mode*) para cifrar un texto pequeño y uno más grande. Se comparó el valor del vector de inicialización para ambos textos y se pudo comprobar que los valores eran diferentes. Puesto que el cifrado en modo CBC supone que el cifrado de cada bloque dependa del contenido del bloque anterior y no solo de su propio contenido. Este vector se utiliza para, como bien indica su nombre, iniciar el cifrado ya que en el primer bloque no hay un bloque previo para utilizar.

Al probar con el cifrado DES en modo ECB (*Code Book Mode*) se pudo comprobar que, tal y como se esperaba dado su comportamiento, el vector inicial no forma parte de los elementos que se utilizan para el cifrado del vector. Este vector no forma parte del encriptado en este modo, puesto que los bloques se cifran individualmente, dependiendo únicamente de sí mismos. Esto provoca una debilidad, ya que las repeticiones en el texto plano, cifradas con la misma clave, que sí que es común a todos los bloques, originan el mismo texto cifrado. Es decir, que en caso de que se intentara producir un ataque, se proveería al atacante con demasiada información.

a. COMPARACIÓN DE LOS RESULTADOS DEL CIFRADO UTILIZANDO DIFERENTES ALGORITMOS SIMÉTRICOS.

Algoritmo	Longitud de clave	Tamaño de bloque	Tamaño de fichero cifrado	Vector de inicialización
DES	56 bits	64 bits	6568 bytes	iv =D3A5D33CD1425C30
3DES	168 bits	64 bits	6568 bytes	iv =8BC3364BCB50829D
AES (128)	128 bits	128 bits	6576 bytes	iv =F6A7A9391A5CBCC851CC027B0070D3FC
AES (192)	192 bits	128 bits	6576 bytes	Iv=D694A171547CDC0829C549E9CDF9486A
AES (256)	256 bits	128 bits	6576 bytes	iv =448D5631B42FC1ABDBD0BB55167AFE0C

b. APLICACIÓN DE UN ALGORITMO DE CIFRADO SIMÉTRICO A UN FICHERO PDF.

- 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.

III. 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?

IV. 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

- *¿Codificación o cifrado? Aclaraciones que marcan la diferencia*. C. Gutiérrez Amaya. 7/12/2016. https://www.welivesecurity.com/la-es/2016/12/07/codificacion-o-cifrado-diferencia/ [Última visita: 19/10/2017]
- *Enc.* OpenSSL. https://wiki.openssl.org/index.php/Enc [Última visita: 19/10/2017]