Seguridad de Sistemas Informáticos - práctica 4

Criptografía simétrica

1. Generar el digesto SHA1 y el digesto MD5 de un archivo de texto utilizando los comandos sha1sum y md5sum respectivamente.

2. Utilizar los mismos comandos para verificar la integridad de los archivos (opción -c)

3. Alterar el archivo agregando un espacio. Generar nuevamente los digestos. Compararlos con los originales.

4. Alterar el archivo cambiando una letra por su sucesora (ej. una 'a' por una 'b'). Generar nuevamente los digestos. Compararlos con los originales.

5. Implementar el comando genhmacmd5 que tome como parámetro dos enteros de 64 bits (que se concatenarán para formar una clave de 128 bits), un texto en claro por entrada estandar y devuelva por salida estandar el digesto md5 generado utilizando el protocolo HMAC. Se recomienda utilizar bash scripting.

   hmac(k1,k2,m) = h(k1 xor o || k2 xor o || o {6 veces} || h(k1 xor i || k2 xor i || i {6 veces} || m))

   donde o=0x5c5c5c5c5c5c5c5c y i=0x3636363636363636

   Referencia echo -n "Hola que tal" | ./genhmacmd5 90 590
   569aa130e17eb9bda040a7fbfe755a9d

6. Utilizar el comando gpg para cifrar simétricamente un archivo de texto utilizando al menos dos algoritmos (ej. AES y 3DES). (opciones `--cipher-algo -c --armour`)

7. Descifrar los archivos anteriores utilizando gpg sin opciones.