Criptografía y Cifrado de Información 2021

Lab 06

07.septiembre.2021

En este laboratorio implementaremos funciones de hash criptográficas de uso común como SHA256 y SHA512, así como mecanismos de códigos de autenticación de mensajes (MAC).

1. Implementar los cifrados sha256, sha512 y blake2b. Para ello, utilizar la librería **hashlib**, la cual ya contiene varias implementaciones de estos cifrados.

   Probar los cifrados anteriores para dos cadenas de texto cortas, produciendo la salida del hash en binario, en hexadecimal, y en base64.

   Modificar los parámetros de *digest_size* en el caso del cifrado blake2b.

2. Simular con las rutinas del ejercicio 1 el proceso de autenticación sobre el contenido de un archivo.
   Aquí deberá implementar una función que, dado un archivo y una clave, genere un hash correspondiente al archivo; además, debe construir una función que reciba como argumentos el archivo, la clave y el hash, y verifique que el hash proporcionado corresponde al archivo.

   a) Genere dos archivos de texto .txt, en donde el segundo archivo sea una copia del primero, únicamente con un caracter modificado (una letra cambiada, o un punto cambiado por una coma, o similar).
   b) Produzca los códigos hash de ambos archivos y verifique que son completamente distintos.
   c) Muestre con dos ejemplo el funcionamiento de la función de verificación: En el primer caso, pase como argumentos el archivo1, la clave y el hash1; en el segundo caso, pase como argumentos el archivo1, la clave, y el hash2 (correspondiente al archivo2).

3. Simular un manejador de passwords, utilizando un esquema hmac, con base en sha256 ó sha512. Puede usar las implementaciones de las librerías **hashlib** o **hmac**.

   En un archivo (puede ser .dat, .csv, .txt u otro formato de su elección), guarde la información siguiente

Usuario	Salt	Hash o Digest
user1	e03d0914b1a7a	k0NcGiKpfrMdVu5yG2UNkMsX2vU1uPjUcnA14cv2ghw=
user2	f24b12507b9bd	h56YnPzjU7T4rDLs6nJVZCvRShKl4VDBrOfNAdm+OHg=
...	...	...

   Debe hacer una función de *Register*, que permita a un usuario nuevo registrarse en su "servidor". El usuario deberá ingresar su nombre de usuario y su password. En su archivo base de datos, usted deberá guardar el nombre del usuario, el salt aleatorio asignado y el hash.

   Debe también crear una función de *Login*, que permita al usuario ingresar con su password. Esta función deberá pedir al usuario que ingrese su nombre de usuario y password. Si se verifica que el hash generado coincide con el guardado en la base de datos, la función debe mostrar un mensaje de bienvenida al usuario. En caso contrario, debe indicar all usuario que su nombre o contraseña son inválidos, y que intente nuevamente.