GENERALITAT VALENCIANA
Conselleria d'Educació, Cultura i Esport

ceedcv CENTRE ESPECÍFIC D'EDUCACIÓ A DISTÀNCIA DE LA COMUNITAT VALENCIANA

Unidad 4.2
Criptografía
Ejercicio evaluable 1

Licencia

1 Hashing MD5

En este ejercicio, se solicita realizar un cambio en el algoritmo de hash de sha1 a md5, ajustando también los comentarios correspondientes en el código existente. La nueva implementación debe interactuar con el usuario de la siguiente manera:

- El programa debe pedir al usuario el nombre del fichero mediante la siguiente instrucción: input("Nombre de fichero: ")
- Posteriormente, se solicita al usuario introducir el código HASH que se desea comprobar con la siguiente instrucción:

  input("Introduce el código HASH a comprobar: ")
- Con base en la entrada proporcionada por el usuario, el código debe imprimir una de las dos opciones siguientes:
  - Si los dos HASH coinciden, se imprime "**Código HASH MD5 correcto**".
  - Si los HASH no coinciden, se imprime "**Código HASH MD5 incorrecto**".

En términos de lógica, el nuevo código debe comparar el HASH introducido por el usuario con el HASH obtenido al realizar el hash del fichero (ver **instrucciones**). La coincidencia de ambos HASH indica que el código HASH es correcto, mientras que la falta de coincidencia indica que el fichero ha sido modificado.

Instrucciones para averiguar el código HASH MD5 del fichero:

Usaremos los comandos que ya llevan integrados la mayoría de sistemas operativos. En este enlace te guía para saber el comando correcto para cada Sistema Operativo:

https://technastic.com/check-md5-checksum-hash/

- **Linux**: md5sum [fichero] o también openssl md5 [fichero]
- **MAC**: md5 [fichero] o también openssl md5 [fichero]
- **Windows**: get-filehash -Algorithm MD5 [fichero]