Name: DJEUTIO QUOIMON ANDERSON ROY

Matricule: FE21A169

IMPLEMENTATION OF MD5 ENCRYPTION FUNCTION

ALGORITHM

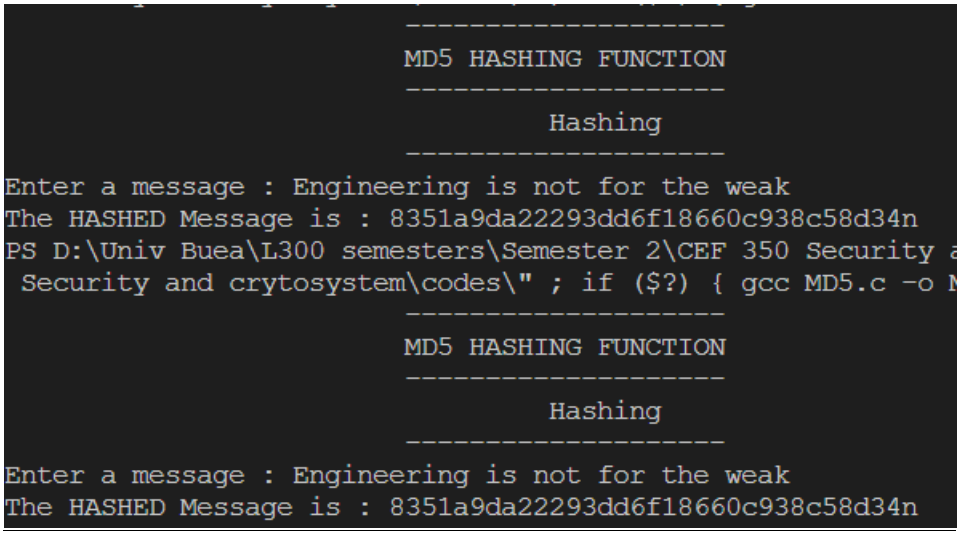
The RIPEMD algorithm is a family of hash functions that produce a fixed-size output from an input message of any length. The RIPEMD-160 variant produces a 160-bit output.

- In this implementation, we define a md5() function that takes in the message to hash, its length, and an array to store the resulting hash.
- I initialized the hash variables h0, h1, h2, and h3 to their initial values, and perform the pre-processing steps required for the MD5 algorithm.
- Then, I process the message in 16-word blocks using the main loop of the MD5 algorithm, and add the resulting hash to the result so far.
- Finally, we output the resulting hash in hexadecimal format.

WORKING PRINCIPLE

It is a sub-block of the RIPEMD-160 hash algorithm. The message is processed by compression function in blocks of 512 bits and passed through two streams of this sub-block by using 5 different versions in which the value of constant ‘k’ is also different.

EXECUTION



The above shows two same messages showing the same hashed outputs