Name: Djeutio Quoimon Anderson Roy

Matricule: FE21A169

IMPLEMENTATION OF RIPEMD ENCRYPTION FUNCTION

ALGORITHM

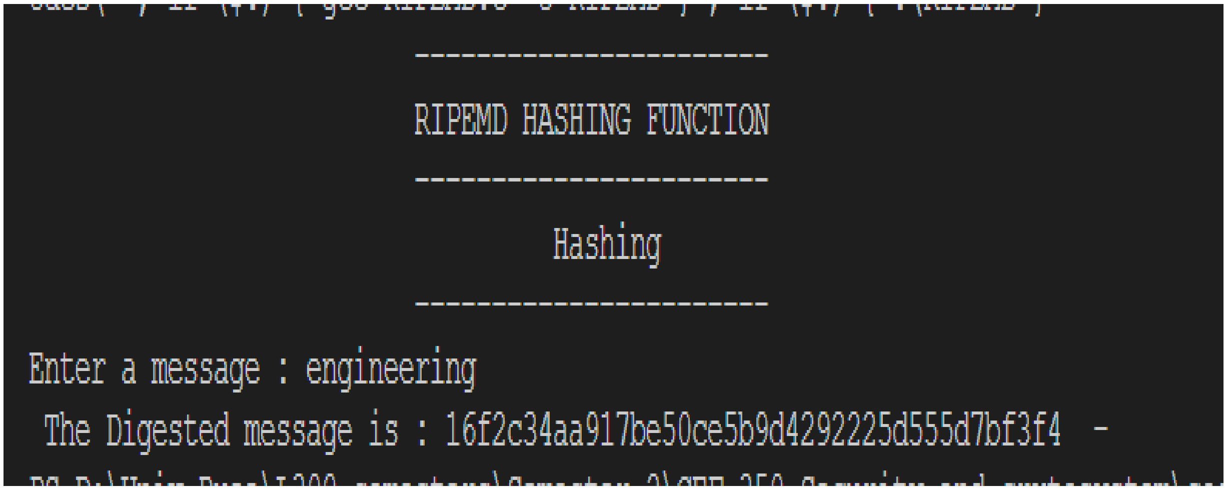
The RIPEMD algorithm is a family of hash functions that produce a fixed-size output from an input message of any length. The RIPEMD-160 variant produces a 160-bit output.

- Parse the input message into blocks of 512 bits.
- Initialize the state of the hash function to a fixed value.
- Process each block of the message using a compression function that updates the state.
- Append the padding bits to the last block of the message.
- Process the last block of the message using the compression function.
- Extract the output from the state.

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



```
 if ($?) { gcc RIPEMD.c -o RIPEMD } ; if ($?) { .\RIPEMD }
                             -----------------------

                             RIPEMD HASHING FUNCTION

                             -----------------------

                                     Hashing

                             -----------------------

Enter a message : engineering
 The Digested message is : 16f2c34aa917be50ce5b9d4292225d555d7bf3f4  -
```