Name: Djeutio Quoimon Anderson Roy

Matricule: FE21A169

IMPLEMENTATION OF SHA-3 ENCRYPTION FUNCTION

ALGORITHM

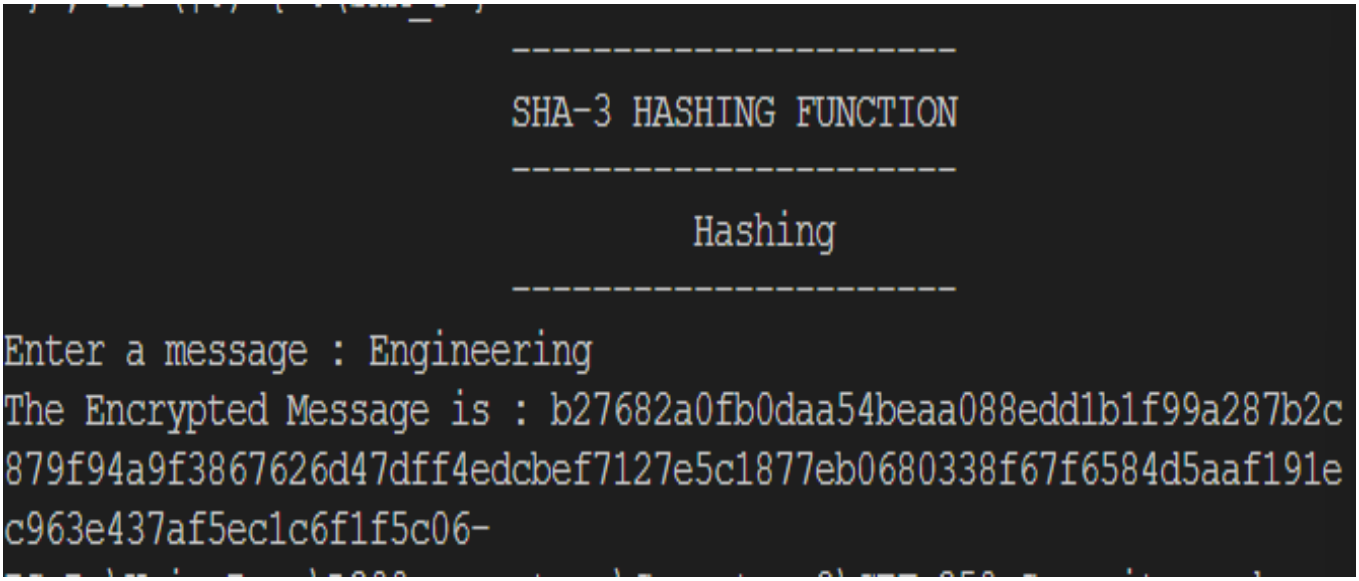
SHA-3 is the latest member of the SHA family and was selected as the winner of the NIST hash function competition. It is designed to be faster and more secure than SHA-2 and produces hash values of 224, 256, 384, and 512 bits.

- Parse the input message into blocks of 1088 bits.
- Initialize the state of the sponge function to a fixed value.
- XOR the first block of the message with the state.
- Apply the permutation function to the state.
- Repeat steps 3 and 4 for all the blocks of the message.
- Append the padding bits to the last block of the message.
- XOR the last block of the message with the state.
- Apply the permutation function to the state.
- Extract the output bits from the state.

WORKING PRINCIPLE

1) The SHA-3 algorithm is based on the Keccak sponge function. The sponge function consists of two main phases: the absorbing phase and the squeezing phase.
   a) In the absorbing phase, the input message is divided into blocks and XORed with the state of the sponge function. The state is then passed through a permutation function, which is a non-linear function that shuffles the bits of the state.
   b) In the squeezing phase, the output is generated by repeatedly applying the permutation function to the state and extracting the output bits.

EXECUTION


SHA-3 HASHING FUNCTION
Hashing
Enter a message : Engineering
The Encrypted Message is : b27682a0fb0daa54beaa088edd1b1f99a287b2c
879f94a9f3867626d47dff4edcbef7127e5c1877eb0680338f67f6584d5aaf191e
c963e437af5ec1c6f1f5c06-