Name :- Gaurang Raorane

Roll No:- 49

Class:- D15A

**Aim:-** Write a Program to implement Cryptographic Hash Functions And Applications (HMAC)

**Input:-**

import hmac

message = input("Enter a message: ")

key = input("Enter an HMAC key: ")

try:

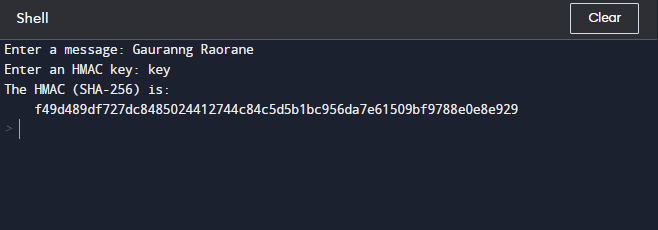
hmac\_digest = hmac.new(key.encode(), message.encode(), "sha256").hexdigest()

print(f"The HMAC (SHA-256) is: {hmac\_digest}")

except Exception as e:

print(e)

**Output:-**



According to the sha256 algorithm a 64 bit output is generated .

**Using md5 as a digestmod**

**Input:-**

import hmac

message = input("Enter a message: ")

key = input("Enter an HMAC key: ")

try:

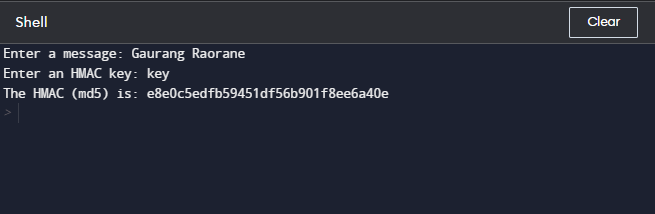
hmac\_digest = hmac.new(key.encode(), message.encode(), "md5").hexdigest()

print(f"The HMAC (md5) is: {hmac\_digest}")

except Exception as e:

print(e)

**Output:-**



A 32 bit output is generated

**Using sha512 as a message digest :-**

**Input:-**

import hmac

message = input("Enter a message: ")

key = input("Enter an HMAC key: ")

try:

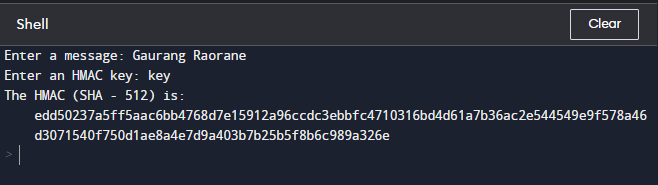
hmac\_digest = hmac.new(key.encode(), message.encode(), "sha512").hexdigest()

print(f"The HMAC (SHA - 512) is: {hmac\_digest}")

except Exception as e:

print(e)

**Output:-**



A 128 bit output is generated.