**Department of Computer Engineering**

**Name of the Student: Parth Das Roll Number: C-111**

**SAP ID: 60004220185 Class: Comps Division: C-2 Batch: 2**

**Subject: Information Security**

**DATE OF PERFORMANCE: 05/04/2025 DATE OF SUBMISION: 05/04/2025**

**EXPERIMENT NO: 7**

**AIM:** To implement Hashing Algorithm using MD5 and SHA1

**Theory:**

**SOURCE CODE WITH OUTPUTS:**

1. **SHA-1**

import hashlib

def hash\_with\_sha1(message):

encoded\_msg = message.encode()

hash\_object = hashlib.sha1(encoded\_msg)

hex\_dig = hash\_object.hexdigest()

return hex\_dig

message = "InformationSecurity123"

hashed\_output = hash\_with\_sha1(message)

print("Original Message:", message)

print("SHA-1 Hashed Output:", hashed\_output)

**Output:-**



1. **MD5:-**

def f(b, c, d):

return hex((int(b, 16) & int(c, 16)) | (~int(b, 16) & int(d, 16)))

text = "Hello my name is Parth Das"

print(f"Plain Text : {text}")

t = [bin(ord(i))[2:] for i in text]

text\_bin = ""

for i in t:

text\_bin += i

len\_text = len(text\_bin)

required\_padding = (512 - 64) - len\_text%512

padded\_text = text\_bin + "1" + "0"\*(required\_padding - 1)

padded\_text = padded\_text + "0"\*(64 - len(bin(len\_text)[2:])) + bin(len\_text)[2:]

A, B, C, D = "0x01234567", "0x89ABCDEF", "0xFEDCBA98", "0x76543210"

a, b, c, d = A, B, C, D

message\_seg = [padded\_text[i : 32+i] for i in range(0, 512, 32)]

keys = ['0xe0a5e0a5', '0x465a465a', '0xf737d44a', '0x6728bd47',

'0xb779d44a', '0x470bd44a', '0x34f2d44a', '0xbd47bd47',

'0xc7ab1a7f', '0xd44ad44a', '0xaa85bd47', '0x1f91d44a',

'0x6e541a7f', '0xdb1f1a7f', '0x13961a7f', '0x1a7f1a7f']

for i in range(16):

f\_bcd = f(b, c, d)

a = hex((int(a, 16) + int(f\_bcd, 16))%(int("0xffffffff", 16)))

a = hex((int(a, 16) + int(message\_seg[i], 2))%(int("0xffffffff", 16)))

a = hex((int(a, 16) + int(keys[i], 16))%(int("0xffffffff", 16)))

a\_bin = bin(int(a, 16))[2:]

a = a\_bin[5:] + a\_bin[:5] # s = 5

a = hex((int(a, 16) + int(b, 16))%int("0xffffffff", 16))

a, b, c, d = d, a, b, c

hash\_message = ""

for i in [a, b, c, d]:

j = i[2:]

hash\_message += "0"\*(4 - len(j)) + i[2:]

print(f"Hased Message(MD5) : {hash\_message}")

**Output:-**



**CONCLUSION:**

MD5 and SHA-1 are widely known cryptographic hash functions used to ensure data integrity. Both algorithms generate a fixed-length hash value for any input, with MD5 producing a 128-bit hash and SHA-1 a 160-bit hash. They were initially trusted for password storage, digital signatures, and file verification. However, due to the discovery of collision vulnerabilities, their security has been significantly compromised.