**AP25122050004**

**Avisikta Mandal Das**

**Cryptography Lab-4 : Authenticating the signature using MD5 hash algorithm**

**Github Link :** [**https://github.com/AvisiktaMandalDas/Cryptography\_Lab4**](https://github.com/AvisiktaMandalDas/Cryptography_Lab4)

**Code:**

import hashlib

def generate\_md5\_signature(message):

"""Generate MD5 hash signature for a given message"""

md5\_hash = hashlib.md5(message.encode())

return md5\_hash.hexdigest()

def verify\_signature(message, signature):

"""Verify if received signature matches the computed hash"""

computed\_hash = hashlib.md5(message.encode()).hexdigest()

if computed\_hash == signature:

print("Signature is authentic. Message integrity verified.")

else:

print(" Signature is invalid. Message may have been altered.")

message = "This is a confidential message."

signature = generate\_md5\_signature(message)

print("Generated Signature:", signature)

verify\_signature(message, signature)

tampered\_message = "This is a modified message." verify\_signature(tampered\_message, signature)

