**ASSIGNMENT NO : 10**

**NAME :** Viraj Patil

**PRN:** 21510097

1. Q - Implement the SIGNATURE SCHEME – Digital Signature Standard**.**

from cryptography.hazmat.primitives.asymmetric import dsa

from cryptography.hazmat.primitives import hashes

private\_key = dsa.generate\_private\_key(key\_size=2048)

message = b"This is a message for digital signature."

signature = private\_key.sign(

message,

hashes.SHA256()

)

print(f"Signature: {signature.hex()}")

public\_key = private\_key.public\_key()

try:

public\_key.verify(

signature,

message,

hashes.SHA256()

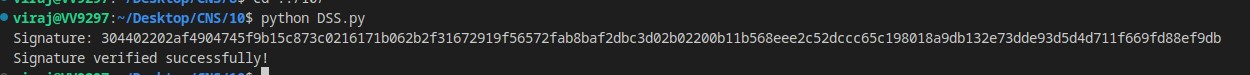
)

print("Signature verified successfully!")

except Exception as e:

print("Signature verification failed:", str(e))

OUTPUT :



Working :

