Nam : Shabbar Adamjee  
Roll No.: PB57  
PRN: 1032221508

*ICS LAB ASSIGNMENT 7*

*DIGITAL SIGNATURE*

*Code*

from cryptography.hazmat.primitives import hashes

from cryptography.hazmat.primitives.asymmetric import padding, rsa

private\_key = rsa.generate\_private\_key(public\_exponent=65537, key\_size=512)

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

message = b"Send dudes"

message2 = b"Send guys"

signature = private\_key.sign(

    message,

    padding.PSS(mgf=padding.MGF1(hashes.SHA256()), salt\_length=padding.PSS.MAX\_LENGTH),

    hashes.MD5(),

)

print(f"Signature: {signature}\n")

try:

    public\_key.verify(

        signature,

        message2,

        padding.PSS(

            mgf=padding.MGF1(hashes.SHA256()), salt\_length=padding.PSS.MAX\_LENGTH

        ),

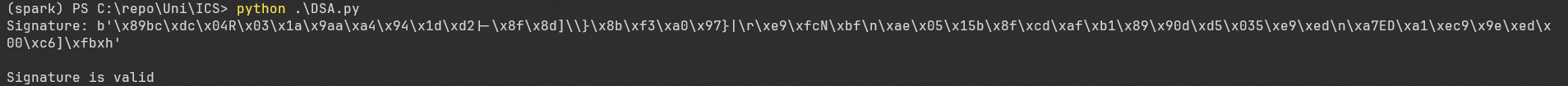
        hashes.MD5(),

    )

    print("Signature is valid")

except Exception as e:

    print("Signature is not valid")

*Output*

