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

ICS LAB ASSIGNMENT 7

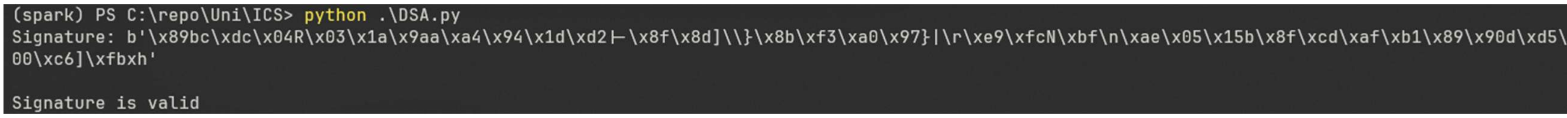
DIGITAL SIGNATURE

Code

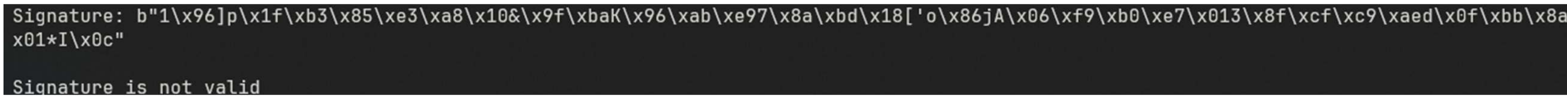
```
from cryptography.hazmat.primitives import hashes
from cryptography.hazmat.primitives.asymmetric import padding, rsa

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")
```

[redacted]

Output



```
(spark) PS C:\repo\Uni\ICS> python .\DSA.py
Signature: b'\x89bc\xdc\x04R\x03\x1a\x9aa\xa4\x94\x1d\xd2⊢\x8f\x8d]\\}\x8b\xf3\xa0\x97}|\r\xe9\xfcN\xbf\n\xae\x05\x15b\x8f\xcd\xaf\xb1\x89\x90d\xd5\
00\xc6]\xfbxh'

Signature is valid
```



```
Signature: b"1\x96]p\x1f\xb3\x85\xe3\xa8\x10&\x9f\xbaK\x96\xab\xe97\x8a\xbd\x18['o\x86jA\x06\xf9\xb0\xe7\x013\x8f\xcf\xc9\xaed\x0f\xbb\x8a
x01*I\x0c"

Signature is not valid
```