Name: Jigar Siddhpura **SAPID:** 60004200155

DIV: C/C2 **Branch:** Computer Engineering

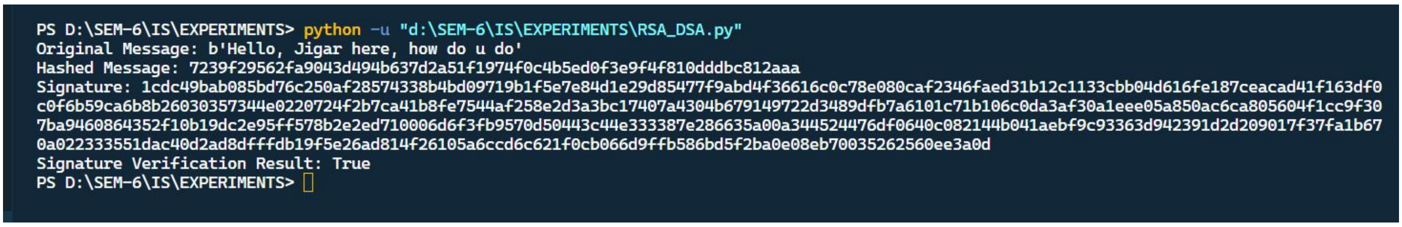
IS - Experiment 8 - SQL Injection

Code :

```
from cryptography.hazmat.backends import default_backend
from cryptography.hazmat.primitives import hashes
from cryptography.hazmat.primitives.asymmetric import padding
from cryptography.hazmat.primitives.asymmetric import rsa

def generate_key_pair():
    private_key = rsa.generate_private_key(
        public_exponent=65537,
        key_size=2048,
        backend=default_backend()
    )
    public_key = private_key.public_key()
    return private_key, public_key

def sign_message(private_key, message):
    signature = private_key.sign(
        message,
        padding.PSS(
            mgf=padding.MGF1(hashes.SHA256()),
            salt_length=padding.PSS.MAX_LENGTH
        ),
        hashes.SHA256()
    )
    return signature

def verify_signature(public_key, message, signature):
    try:
        public_key.verify(
            signature,
            message,
            padding.PSS(
                mgf=padding.MGF1(hashes.SHA256()),
                salt_length=padding.PSS.MAX_LENGTH
            ),
            hashes.SHA256()
        )
        return True
    except Exception as e:
        print(f"Signature verification failed: {e}")
        return False

private_key, public_key = generate_key_pair()
message = b"Hello, Jigar here, how do u do"
print("Original Message:", message)

digest = hashes.Hash(hashes.SHA256(), backend=default_backend())
digest.update(message)
hashed_message = digest.finalize()
print("Hashed Message:", hashed_message.hex())

signature = sign_message(private_key, hashed_message)
```

```
print("Signature:", signature.hex())

verification_result = verify_signature(public_key, hashed_message, signature)
print("Signature Verification Result:", verification_result)
```

Output :



```
PS D:\SEM-6\IS\EXPERIMENTS> python -u "d:\SEM-6\IS\EXPERIMENTS\RSA_DSA.py"
Original Message: b'Hello, Jigar here, how do u do'
Hashed Message: 7239f29562fa9043d494b637d2a51f1974f0c4b5ed0f3e9f4f810dddbc812aaa
Signature: 1cdc49bab085bd76c250af28574338b4bd09719b1f5e7e84d1e29d85477f9abd4f36616c0c78e080caf2346faed31b12c1133cbb04d616fe187ceacad41f163df0
c0f6b59ca6b8b26030357344e0220724f2b7ca41b8fe7544af258e2d3a3bc17407a4304b679149722d3489dfb7a6101c71b106c0da3af30a1eee05a850ac6ca805604f1cc9f30
7ba9460864352f10b19dc2e95ff578b2e2ed710006d6f3fb9570d50443c44e333387e286635a00a344524476df0640c082144b041aebf9c93363d942391d2d209017f37fa1b67
0a022333551dac40d2ad8dfffdb19f5e26ad814f26105a6ccd6c621f0cb066d9ffb586bd5f2ba0e08eb70035262560ee3a0d
Signature Verification Result: True
PS D:\SEM-6\IS\EXPERIMENTS> 
```