Neha Dattatray Bhoite

Assignment No 5 -

1)RSA Algorithm

```
from Crypto.PublicKey import RSA
from Crypto.Cipher import PKCS1_OAEP
import binascii
def generate_keys():
    key = RSA.generate(2048)
    private_key = key.export_key()
    public_key = key.publickey().export_key()
    return private_key, public_key
def rsa_encrypt(public_key, plaintext):
    recipient_key = RSA.import_key(public_key)
    cipher_rsa = PKCS1_OAEP.new(recipient_key)
    encrypted_text = cipher_rsa.encrypt(plaintext.encode())
    return binascii.hexlify(encrypted_text).decode()

def rsa_decrypt(private_key, ciphertext):
    private_key = RSA.import_key(private_key)
    cipher_rsa = PKCS1_OAEP.new(private_key)
    decrypted_text = cipher_rsa.decrypt(binascii.unhexlify(ciphertext)).decode()
    return decrypted_text

# Generate RSA key pair
private_key, public_key = generate_keys()
# Example usage
plaintext = "HelloRSA123"
ciphertext = rsa_encrypt(public_key, plaintext)
decrypted_text = rsa_decrypt(private_key, ciphertext)

print(f"Plaintext: {plaintext}")
print(f"Ciphertext: {ciphertext}")
print(f"Decrypted Text: {decrypted_text}")
```

Output-

```
Plaintext: HelloRSA123
Ciphertext:
8f3c7e5a9d2b1c4e6f7a8b9c0d1e2f3a4b5c6d7e8f9a0b1c2d3e4f5a6b7c8d9e  #
(Example, will vary)
Decrypted Text: HelloRSA123
```