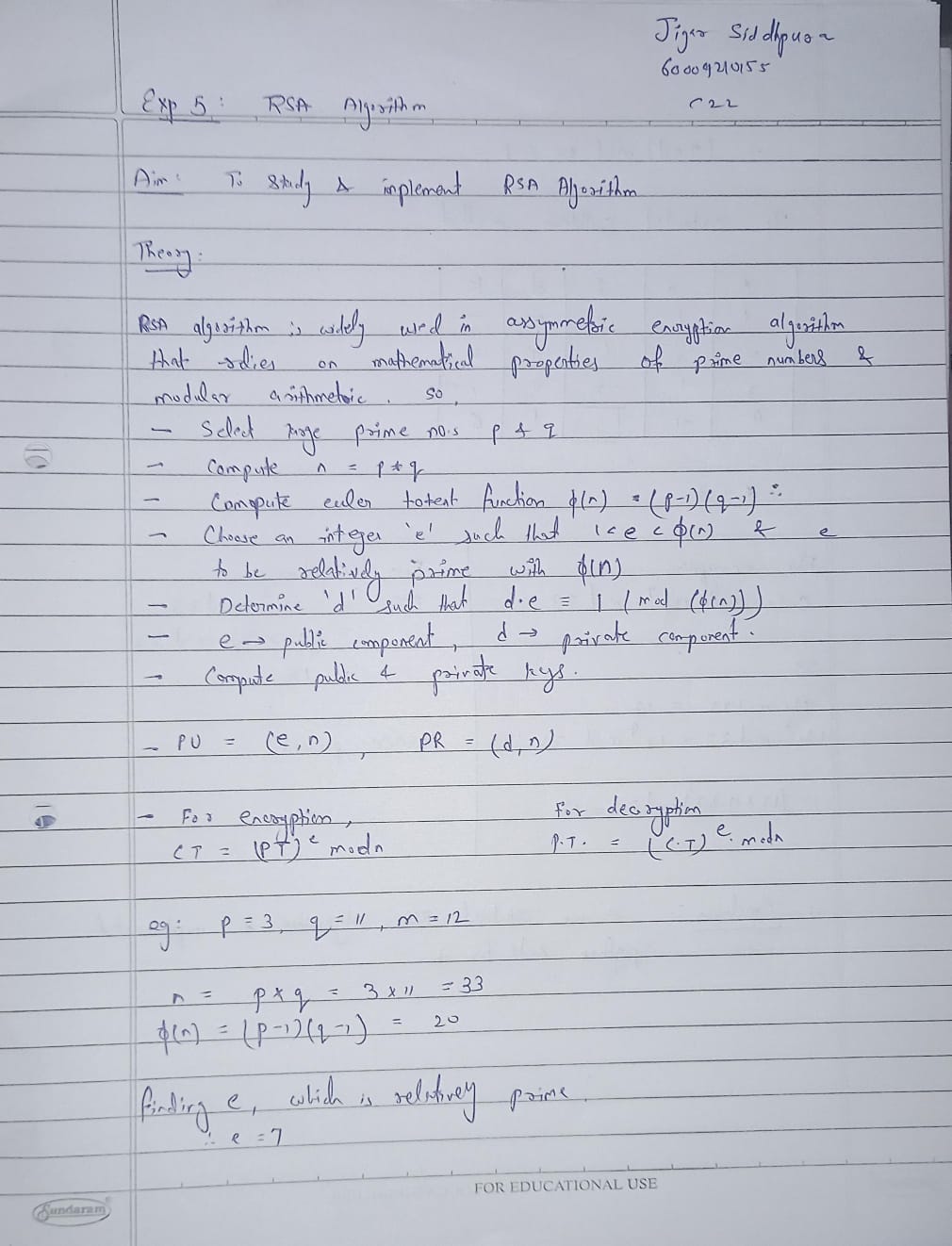
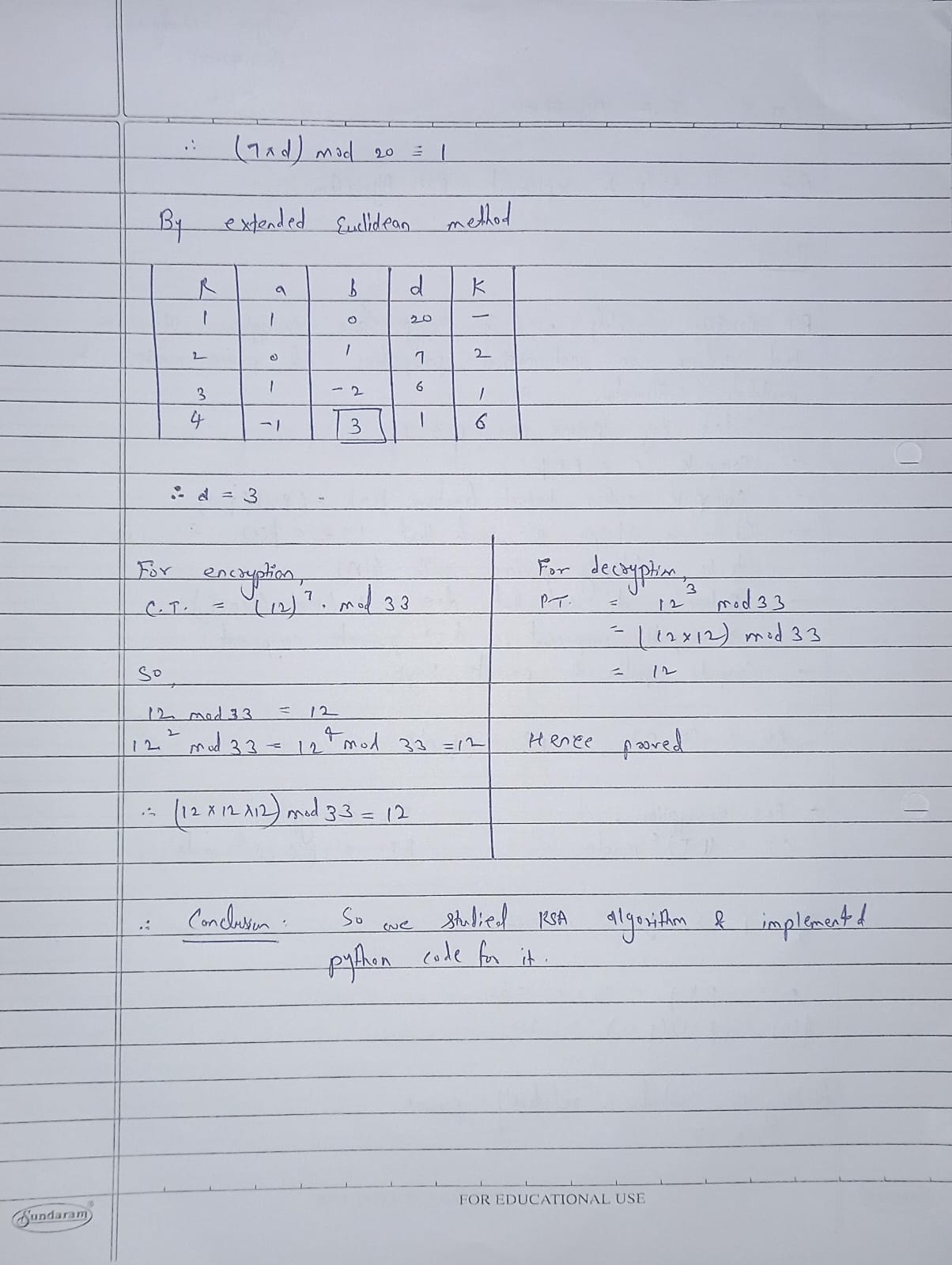
**Name: Jigar Siddhpura SAPID:** 60004200155

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

IS - Experiment 5 - RSA ALGORITHM





**CODE**

# Get prime numbers p and q

p = int(input("Enter p (prime number): "))

q = int(input("Enter q (prime number): "))

# Get public exponent e that is relatively prime to (p-1)\*(q-1)

e = int(input(f"Enter e (relatively prime to {(p-1)\*(q-1)}): "))

# Calculate n and φ(n)

n = p \* q

phi = (p - 1) \* (q - 1)

# Calculate private exponent d

d = 1

while True:

    if (d \* e) % phi == 1:

        break

    d += 1

msg\_length = int(input("Enter the length of the message (in bits): "))

print(f"p: {p}, q: {q}, message bits: {msg\_length}, e: {e}")

print(f"Public key: {(e, n)}\nPrivate Key: {(d, n)}\n")

msg\_data = int(input("Enter the message data: "))

print("Message data = ", msg\_data)

encrypted\_data = (msg\_data \*\* e) % n

print("Encrypted data = ", encrypted\_data)

decrypted\_data = (encrypted\_data \*\* d) % n

print("Original Message Sent = ", decrypted\_data)

**OUTPUT**

