import math

# Step 1: Get two prime numbers

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

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

# Step 2: Calculate n and phi

n = p \* q

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

# Step 3: Find e (public key exponent)

e = 2

while e < phi:

    if math.gcd(e, phi) == 1:

        break

    e += 1

# Step 4: Find d (private key exponent)

k = 2

d = ((k \* phi) + 1) // e

# Step 5: Show the keys

print("\nPublic key: (", e, ",", n, ")")

print("Private key: (", d, ",", n, ")\n")

# Step 6: Get message from the user

msg = int(input("Enter a number message to encrypt (less than n): "))

if msg >= n:

    print("Message should be less than n. Please try again.")

else:

    # Step 7: Encrypt the message

    C = pow(msg, e, n)

    print("Encrypted message:", C)

    # Step 8: Decrypt the message

    M = pow(C, d, n)

    print("Decrypted message:", M)