Step 1: Start

Step 2: Input Primes and Message:

2.1:Prompt "Enter prime numbers p and q" and store them as p and q.

2.2:Prompt "Enter the number" to encrypt and store it as M.

print("Enter prime numbers p and q: ")

p, q = user input

print("Enter the number: ")

M = user input

Step 3: Calculate RSA Parameters:

3.1:Compute n as p * q.

3.2:Compute phi as (p - 1) * (q - 1).

n = p * q

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

Step 4: Find Public Key Exponent e:

4.1:Starting from e = 2, find the smallest integer e such that gcd(e, phi) = 1.

Step 5: Calculate Private Key Exponent d:

5.1:Find d such that (e * d) % phi = 1.

while (e * d) % phi != 1:

d = d + 1

Step 6: Encrypt the Message:

6.1:Calculate the encrypted message using modular exponentiation: M^e % n.

encrypted = (M^e) % n

Step 7: Display Encrypted Message:

7.1:Print the encrypted message.

Step 8: Decrypt the Message:

8.1:Calculate the decrypted message using modular exponentiation: encrypted^d % n.

Step 9: Display Decrypted Message:

9.1:Print the decrypted message, confirming it matches M.

Step 10: Stop