

24. Write a python program for RSA system, the public key of a given user is $e = 31$, $n = 3599$. What is the private key of this user? Hint: First use trial-and-error to determine p and q ; then use the extended Euclidean algorithm to find the multiplicative inverse of 31 modulo $f(n)$.

```
# RSA key recovery and simple demo for n=3599, e=31
```

Code:

```
def trial_factor(n):  
    # simple trial division (works fast for a small n like 3599)  
  
    i = 2  
  
    while i * i <= n:  
        if n % i == 0:  
            return i, n // i  
  
        i += 1 if i == 2 else 2 # skip even numbers after 2  
  
    return n, 1 # n is prime  
  
def egcd(a, b):  
    # extended Euclidean algorithm  
  
    if b == 0:  
        return (a, 1, 0)  
  
    g, x1, y1 = egcd(b, a % b)  
  
    x = y1  
  
    y = x1 - (a // b) * y1  
  
    return (g, x, y)  
  
def modinv(a, m):  
    g, x, y = egcd(a, m)  
  
    if g != 1:  
        raise ValueError("Modular inverse does not exist")  
  
    return x % m  
  
def rsa_recover_private(e, n):  
    p, q = trial_factor(n)  
  
    if p * q != n:
```

```
raise ValueError("Failed to factor n with simple trial division.")

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

d = modinv(e, phi)

return (p, q, phi, d)

def rsa_encrypt(m, e, n):

    return pow(m, e, n)

def rsa_decrypt(c, d, n):

    return pow(c, d, n)

# Given public key

e = 31

n = 3599

p, q, phi, d = rsa_recover_private(e, n)

print("p =", p)

print("q =", q)

print("phi(n) =", phi)

print("private exponent d =", d)

# quick demo: encrypt/decrypt a small integer message (must be < n)

message = 42

cipher = rsa_encrypt(message, e, n)

plain = rsa_decrypt(cipher, d, n)

print("\nDemo:")

print("message =", message)

print("ciphertext =", cipher)

print("decrypted =", plain)
```

The screenshot shows a Python shell window titled "IDLE Shell 3.14.0". The menu bar includes File, Edit, Shell, Debug, Options, Window, and Help. The main window displays the following Python session:

```
Python 3.14.0 (tags/v3.14.0:ebf955d, Oct  7 2025, 10:15:03) [MSC v.1944 64 bit (AMD64)] on win32
Enter "help" below or click "Help" above for more information.

>>> ===== RESTART: C:/Users/Maria/OneDrive/Documents/ex24.py =====
p = 59
q = 61
phi(n) = 3480
private exponent d = 3031

Demo:
message = 42
ciphertext = 2543
decrypted = 42
>>> $
```