16) Write a C 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).

PROGRAM:-

```
def gcd_extended(a, b):
    """Extended Euclidean Algorithm to find the inverse of a modulo b"""
    if a == 0:
        return b, 0, 1
    gcd, x1, y1 = gcd_extended(b % a, a)
    x = y1 - (b // a) * x1
    y = x1
    return gcd, x, y

def mod_inverse(e, phi):
    """Finds modular inverse of e mod phi"""
    gcd, x, _ = gcd_extended(e, phi)
    if gcd != 1:
        raise Exception("Modular inverse does not exist")
    else:
        return x % phi

# Step 1: Trial-and-error to factor n = 3599
n = 3599
for i in range(2, int(n**0.5) + 1):
    if n % i == 0:
        p = i
        q = n // i
        break

print(f"Found primes: p = {p}, q = {q}")
```

```
# Step 2: Compute phi(n)
phi = (p - 1) * (q - 1)
print(f"phi(n) = {phi}")

# Step 3: Given e = 31, find private key d
e = 31
d = mod_inverse(e, phi)
print(f"Private key d = {d}")
```

OUTPUT:-

```
Found primes: p = 59, q = 61
phi(n) = 3480
Private key d = 3031
```
