

## Factor's:

```
def extended_gcd(a, b):
    x0, x1, y0, y1 = 1, 0, 0, 1
    while b != 0:
        q, a, b = a // b, b, a % b
        x0, x1 = x1, x0 - q * x1
        y0, y1 = y1, y0 - q * y1
    return a, x0, y0

def mod_inverse(a, m):
    g, x, y = extended_gcd(a, m)
    if g != 1:
        raise Exception('Modular inverse does not exist')
    else:
        return x % m

# Given values
n = ...
e = 65537
c = ...

# Factorized primes
p = 15485863
q =
2638400886709174529463335454783521274169141667309744459487196170860689
8246191631284922865941012124184327243247514562575750057530808887589809
8480894611741004217089821840822946755005773362259577979888187213725467
4913138087656613760703630147343576403165908527615990944725582431699173
1559776281695919056426990285120277950325598700770588152330565774546219
6113601677479009675113787095763660567278662393597444843430993224406744
3402087420059404103392620257894150896959622939815996558152132664311513
7

# Verify that n = p * q
if n != p * q:
    print("Error: n != p * q")
exit(1)

# Compute Euler's totient function
phi = (p - 1) * (q - 1)

# Compute the private key d
d = mod_inverse(e, phi)

# Decrypt the message
m = pow(c, d, n)

# Convert the message to bytes (assuming it's a string of bytes)
```

```
message = m.to_bytes((m.bit_length() + 7) // 8, 'big')  
print(message.decode())
```

Final FLAG:

flag{kiet\_sh0uld'v3\_t4k3n\_b1gg3r\_pr1m3s\_xd}