

### **Step 1 (Finding p):**

The description hints towards a very famous sequence being used to generate a number, the sequence is Fibonacci and we know that the method called finds the 738th Fibonacci number which is

76452818786420744855351332059441727511430113848087681931773758096200  
95682060320826830288084383872992695342808879708252367835721240788872  
451903860114461144.

Because we have a ciphertext of 1024 bit and so the value of N also has to be 1024 bits and since q is defined to have a width of 512 bits p should also be 512 bits and if we check the 738th Fibonacci number is 512 bits as well and then finds its next prime as hinted by the name of the method "next\_prime\_after".

Now to find p we can simply run:

```
from sympy import Fibonacci, nextprime
fibonum = fibonacci(738)
p = nextprime(fibonum)
print(p)
```

This will give us:

p=7645281878642074485535133205944172751143011384808768193177375809  
620095682060320826830288084383872992695342808879708252367835721240  
788872451903860114461247.

### **Step 2 (Finding q):**

The seed required calls a method what\_cipher\_is\_this and has a hint following it which is r85494729667706749738844398777564856494539744563e

On separating it “rome 8549472966776749738844398777564856494539744563” we can see rome seems to be the key used to encrypt the numbers.

Using the hint given “Maybe The Histories hold a clue” along with the fact that the key is rome and the numbers look like a Alphanumeric Cipher that the cipher being used is Polybius or one of its variants like Nihilist which is a key based cipher that we will use to decrypt the numbers.

On decrypting 8549472966776749738844398777564856494539744563 using the key rome and the default word set “abcdefghijklmnopqrstuvwxyz (-j)” we get seed is polybius in decimal.

Therefore, the seed is 8079768966738583 which is the decimal form of the ASCII Polybius.

Then we see that we perform a method called MR on it which on analyzing has a small puzzle in it after a little investigation we can decrypt is using base 64 and rotation cipher with a shift of 7, we will get the text

"There once was a genius named Fermat who proposed little theorems; three centuries later Carmichael discovered their limitations and under a century after that, those limitations were finally overcome by a Prime suspect."

on solving this clue we discover the prime suspect is the Miller Rabin primality theorem which was used to overcome the Carmichael number limitation in Fermat's little theorem, Miller Rabin is basically a next prime checker for big numbers so we can run:

```
import random
from sympy import nextprime

p =
764528187864207448553513320594417275114301138480876819317737580962
009568206032082683028808438387299269534280887970825236783572124078
8872451903860114461247
seed = 8079768966738583
q = gen_q(p,seed,width)

def gen_q(p, seed, width=512):
    bin_p = bin(p)[2:].zfill(width)
    rev_p = int(bin_p[::-1], 2)

    rnd = random.Random(seed)
    mask = rnd.getrandbits(width)

    candidate = rev_p ^ mask

    if candidate % 2 == 0:
        candidate += 1

    q = nextprime(candidate)
    return q
print(q)
```

We get,

```
q=2014676602493966179691539821190027762577831893539648655842945
522209698645363272966643867723495326883852835245572863900470480317
505860751196570268620469
```

**Step 3 (getting plaintext):**

Now that we have p and q we can simply run:

```
e = 65537
p=7645281878642074485535133205944172751143011384808768193177375809
620095682060320826830288084383872992695342808879708252367835721240
788872451903860114461247
q=2014676602493966179691539821190027762577831893539648655842945
522209698645363272966643867723495326883852835245572863900470480317
505860751196570268620469
N=p*q
ct=748103634940098591938102480237670663003366502180831992090424449
502937657833049911767785707418871868359906140973568479820671739392
019719171210007947043786506667195542060091777371587252491767732487
490699485623578857562414743984287562982571846683450667575413052467
438334899808575341100878805657849318808957256
phi = (p-1)*(q-1)
d = pow ( e, -1, phi)
pt_int = pow( ct, d, N)
pt_bytes = pt_int.to_bytes((pt_int.bit_length() + 7) // 8, "big")
pt = pt_bytes.decode("utf-8")
print(pt)
```

Which will give us the flag “DJSISACA{7h3\_St0rY\_H45\_jU5T\_13eGuN}”.