Description

I just recently learnt about the SRA public key cryptosystem... or wait, was it supposed to be RSA? Hmmm, I should probably check...Connect to the program on our server: `nc saturn.picoctf.net 50372` Download the program: chal.py

Hints

- (None)

Solución

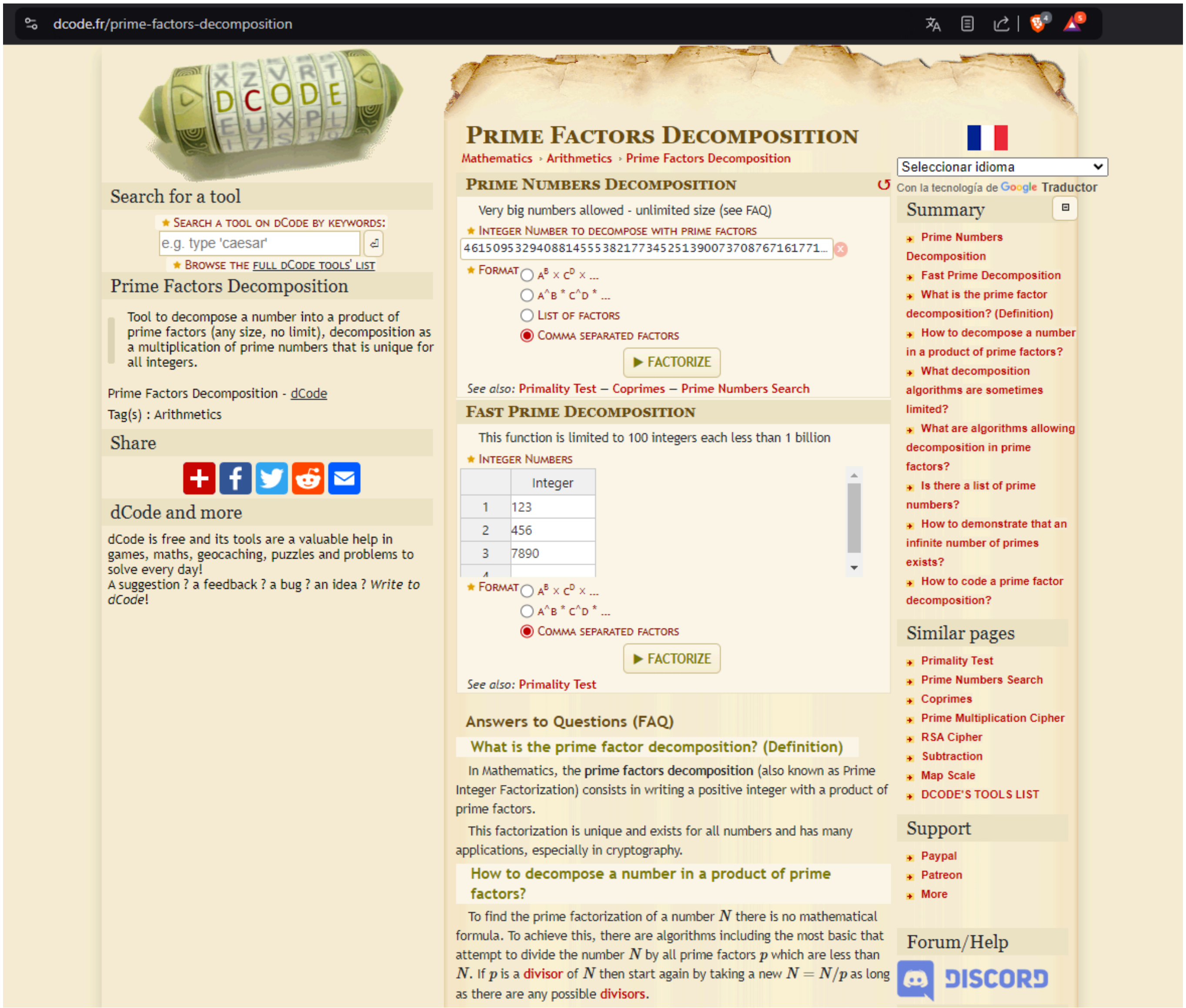
```
from pwn import *
import primefac
from itertools import combinations
from Crypto.Util.number import long_to_bytes

def sub_lists(l):
    comb = []
    for i in range(1,len(l)+1):
        comb += [list(j) for j in combinations(l, i)]
    return comb

def divisors(phi):
    print("Give me the divisors of ", phi-1)
    return(eval(input()))

r = remote('nc saturn.picoctf.net', 50372)
r.recvuntil("anger =")
ciphertext = int(r.recvline())
r.recvuntil("envy =")
d = int(r.recvline())
print("cipher=", ciphertext)
print("d=",d)
print(r.recvuntil("vainglory?"))
r.recvline()
factors=divisors(d*65537)
combos = sub_lists(factors)
primes = set()
for l in combos:
    product = 1
    for k in l:
        product = product * k
    if product.bit_length() == 128 and primefac.isprime(product+1):
        primes.add(product+1)
print(primes)
primelist = list(primes)
for p in primelist:
    for q in primelist:
        n = p*q
        plain = pow(ciphertext,d,n)
        try:
            plaintext = long_to_bytes(plain)
            print(plaintext.decode())
            r.sendline(plaintext.decode())
            print(r.recvline())
            print(r.recvline())
            print(r.recvline())
        except:
            continue
```

```
Mexidis-picoctf@webshell:~/picoCTF/sra$ python3 solve.py
[+] Opening connection to saturn.picoctf.net on port 56935: Done
/home/Mexidis-picoctf/picoCTF/sra/solve.py:17: BytesWarning: Text is not
bytes; assuming ASCII, no guarantees. See https://docs.pwntools.com/#bytes
  r.recvuntil("anger =")
/home/Mexidis-picoctf/picoCTF/sra/solve.py:19: BytesWarning: Text is not
bytes; assuming ASCII, no guarantees. See https://docs.pwntools.com/#bytes
  r.recvuntil("envy =")
cipher=
1721940064957104191966230824124450957250236348295793935901173918088635468278
9
d=
7041969161555784603174050300214214983457843907673303603596612735138810213573
/home/Mexidis-picoctf/picoCTF/sra/solve.py:23: BytesWarning: Text is not
bytes; assuming ASCII, no guarantees. See https://docs.pwntools.com/#bytes
  print(r.recvuntil("vainglory?"))
b'vainglory?'
Give me the divisors of
4615095329408814555382177345251390073708767161771852982689112088227922049669
33700
[2, 2, 3, 3, 3, 5, 5, 7, 7, 11, 19, 73, 3967, 428693, 925823,
2614359612359819, 20458581099053479, 2715027868783753446718259]
{225078752573580492316676853836043318469,
202951020407284451983048426057859074909,
190114373450651243259933449013091225351,
286635704044555119274838993035448353067,
258281645379443661118989299606905513951,
29408052601233615238745821440173609686 3,
```



dcode.fr/prime-factors-decomposition

Prime Factors Decomposition

Mathematics › Arithmetics › Prime Factors Decomposition

Prime Numbers Decomposition

Very big numbers allowed - unlimited size (see FAQ)

★ Integer Number to decompose with prime factors

4615095329408814555382177345251390073708767161771…

★ Format ○ $A^B \times C^D \times$ …
○ A^B * C^D * …
○ List of factors
● Comma separated factors

▶ FACTORIZE

See also: Primality Test – Coprimes – Prime Numbers Search

Fast Prime Decomposition

This function is limited to 100 integers each less than 1 billion

★ Integer Numbers

	Integer
1	123
2	456
3	7890
4	

★ Format ○ $A^B \times C^D \times$ …
○ A^B * C^D * …
● Comma separated factors

▶ FACTORIZE

See also: Primality Test

Answers to Questions (FAQ)

What is the prime factor decomposition? (Definition)

In Mathematics, the **prime factors decomposition** (also known as Prime Integer Factorization) consists in writing a positive integer with a product of prime factors.

This factorization is unique and exists for all numbers and has many applications, especially in cryptography.

How to decompose a number in a product of prime factors?

To find the prime factorization of a number N there is no mathematical formula. To achieve this, there are algorithms including the most basic that attempt to divide the number N by all prime factors p which are less than N. If p is a divisor of N then start again by taking a new $N = N/p$ as long as there are any possible divisors.

Search for a tool
★ Search a tool on dCode by keywords:
e.g. type 'caesar'
★ Browse the full dCode tools' list
Prime Factors Decomposition
Tool to decompose a number into a product of prime factors (any size, no limit), decomposition as a multiplication of prime numbers that is unique for all integers.
Prime Factors Decomposition - dCode
Tag(s) : Arithmetics
Share
dCode and more
dCode is free and its tools are a valuable help in games, maths, geocaching, puzzles and problems to solve every day!
A suggestion ? a feedback ? a bug ? an idea ? Write to dCode!
Seleccionar idioma
Con la tecnología de Google Traductor
Summary
Prime Numbers Decomposition
Fast Prime Decomposition
What is the prime factor decomposition? (Definition)
How to decompose a number in a product of prime factors?
What decomposition algorithms are sometimes limited?
What are algorithms allowing decomposition in prime factors?
Is there a list of prime numbers?
How to demonstrate that an infinite number of primes exists?
How to code a prime factor decomposition?
Similar pages
Primality Test
Prime Numbers Search
Coprimes
Prime Multiplication Cipher
RSA Cipher
Subtraction
Map Scale
DCODE'S TOOLS LIST
Support
Paypal
Patreon
More
Forum/Help
DISCORD

Bandera

```
flag: picoCTF{7h053_51n5_4r3_n0_m0r3_38268294}
```

Notas Adicionales

Para poder resolver este reto se utilizó el webshell de la página de picoCTF para poder utilizar las librerías de python que no funcionan en kali linux.

Referencias

-