Sharif University CTF 2016 - Smooth As Silk

Category: Crypto **Points:** 200 **Solves:** 11
Description:

> p > q
>
> n = p*q =
> 114615328185252517758699943699566283254374785104852727304198433205179406018085975529256294517956119903726515687701818722825903098941878150911916499148332748054194325253862348764773074723370269667454085070040009481121919737770904075581620185589455966913229094043074200945846061032064904265517459102681383938040436418768165985990648563582666503391786171498330323093798580597291798574197510931382958630348442538279 63
>
> flag = md5(str(p))

EN:

Can solve it by using Pollard P-1 Factorization Method（http://www.mersennewiki.org/index.php/P-1_Factorization_Method）;

$$E = 2^{E_2 * 3^{E_3 * 5^{E_5 * \ldots * B}}}$$

step 01:select B1

N =p*q (p>q)

q<=sqrt(N)
B1=sqrt(N)

more B1 is bigger, the more possible can find out it(?! maybe, No!)

step 02: count out E2, E3,E5 ....

我的标签

ctf(13)
writeup(12)
HackIM 2016(10)
nullcon(10)
SharifCTF2016(3)
wechall(1)
Reverse(1)
math(1)
exploiting(1)
Android(1)
更多

随笔分类

CTF(13)
wechall(4)
writeup(13)

随笔档案

2016年2月 (13)
2016年1月 (4)

阅读排行榜

1. Sharif University CTF 2016 -- Android App(309)
2. Sharif University CTF 2016 - Smooth As Silk(284)
3. Sharif University CTF 2016 -- Login to System (PWN 200)(195)
4. nullcon HackIM 2016 -- Crypto Question 5(106)
5. nullcon HackIM 2016 -- Crypto Question 4(84)

$2^{E2}<=B1$, $3^{E3}<=B1$ ...

E2=log(B1)/log(2)

E3=log(B1)/log(3)

E5=log(B1)/log(5)

E7=log(B1)/log(7)

...

push 2 in the z[] E2 times, push 3 in the z[] E3 times, push 5 in the z[] E5 times ...

step 03:

x=a, (a is a prime)

i=0

do

$x^{z[i]}\equiv a \pmod n$

x=a

until gcd(n, x-1) !=1

gcd(n,x-1) is one factor of N.

```
#!/usr/bin/python3
import math

n=114615328185252517758699943699566283254374785104852727304198433205179406018085975529256294517956119903726515687701818722825903098941878150911916499148332748054194325253862348764773074723370269667454085070040009481121919737770904075581620185589455966913229094043074200945846061032064904265517459102681383938040436418768165985990648563582666503391786171498330323093798580597291798574197510931382958630348442538279 63
z=[]
prime=
[2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97,101,103,107,109,113,127,131,137,139,149,151,157,163,167,173,179,181,191,193,197,199,211,223,227,229,233,239,241,251,257,263,269,271,277,281,283,293,307,311,313,317,331,337,347,349,353,359,367,373,379,383,389,397,401
```

```
337,347,349,353,359,367,373,379,383,389,397,401,
409,419,421,431,433,439,443,449,457,461,463,467,
479,487,491,499,503,509,521,523,541,547,557,563,
569,571,577,587,593,599,601,607,613,617,619,631,
641,643,647,653,659,661,673,677,683,691,701,709,
719,727,733,739,743,751,757,761,769,773,787,797,
809,811,821,823,827,829,839,853,857,859,863,877,
881,883,887,907,911,919,929,937,941,947,953,967,
971,977,983,991,997];
def gcd(a,b):
    if b==0:
        return a
    return gcd(b,a%b)

def e(a,b):
    return pow(a,b)%n

def mysqrt(n):
    x=n
    y=[]
    while(x>0):
        y.append(x%100)
        x=x//100
    y.reverse()
    a=0
    x=0
    for p in y:
        for b in range(9,-1,-1):
            if(((20*a+b)*b)<=(x*100+p)):
                x=x*100+p - ((20*a+b)*b)
                a=a*10+b
                break

    return a

B1=mysqrt(n)
for j in range(0,len(prime)):
    for i in range(1,
int(math.log(B1)/math.log(prime[j]))+1):
        z.append(prime[j])

#print(z)

for pp in prime:
    i=0
    x=pp
    while(1):
        x=e(x,z[i])
        i=i+1
        y=gcd(n,x-1)
        if(y!=1):
```

```
                print (y)
                exit(0)
            if(i>=len(z)):
                break
```

python3 sss.py, we can the number:

958483424448747472504060861580795018746355733561446016442794600533395417361061386707061258449029078376132360127073305093209304646989718030495000998517698501250000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001

then

n=114615328185252517758699943699566283254374785104852727304198433205179406018085975529256294517956119903726515687701818722825903098941878150911916499148332748054194325253862348764773074723370269667454085070040009481121919737770904075581620185589455966913229094043074200945846061032064904265517459102681383938040436418768165985990648563582666503391786171498330323093798580597291798574197510931382958630348442538279 63

p=958483424448747472504060861580795018746355733561446016442794600533395417361061386707061258449029078376132360127073305093209304646989718030495000998517698501250000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001

q=119579875104435140490476967855872347582271533733635898918768165985990648563582666503391786171498330323093798580597291798574197510931382958630348442538279 63

flag=md5(str(p)) =
c78504a558bdb6213b9019f6925fa4ae

flag is c78504a558bdb6213b9019f6925fa4ae

CN:

这个是因子分解，用 Pollard P-1因子分解法（http://www.mersennewiki.org/index.php/P-1_Factorization_Method），pyhton3 源码看上面。

还是要看B1的选择，选择不好也是有可能解不出，解不出就重新选择，直到解出。

分类: CTF,writeup

标签: ctf, SharifCTF2016, math

我怎么能不努力奋斗
关注 - 0
粉丝 - 1
+加关注

« 上一篇: Sharif University CTF 2016 -- Login to System (PWN 200)

posted on 2016-02-09 13:02 我怎么能不努力奋斗 阅读(284) 评论(0) 编辑 收藏