

## Big exponent

Đặt  $rnew = r - 1 \rightarrow r = rnew + 1$  thì thuật toán sẽ như sau:

### Tạo khóa:

1. Chọn một số lẻ  $rnew$  ngẫu nhiên  $3 \leq rnew < 2^{b/2}$ .
2. Chọn 2 số nguyên tố  $p, q$  với  $\gcd(p-1, rnew) = 1$  và  $\gcd(q-1, rnew) = 1$ .
3. Tính  $N = p \cdot q$ .
4. Tính  $e = rnew + (p-1) \cdot (q-1)$

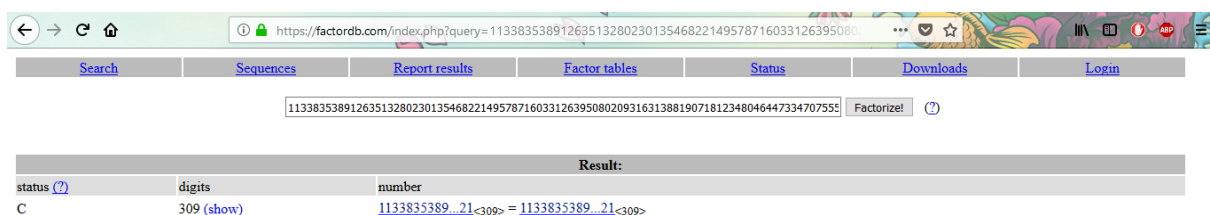
Theo Định lý Fermat có  $m^{p-1} \equiv 1 \pmod{p}$ ,  $m^{q-1} \equiv 1 \pmod{q} \rightarrow m^{(p-1)(q-1)} \equiv 1 \pmod{N} \rightarrow c = m^{rnew} \% N$ . Do vậy hàm transform sẽ không có ý nghĩa gì nữa. Thuật toán mã hóa sẽ như sau:

### Mã hóa:

$\text{cipher}[0] = (\text{block}[0])^e \pmod{N}$   
 $\text{cipher}[1] = (\text{cipher}[0] \cdot \text{block}[1])^e \pmod{N}$   
...  
 $\text{cipher}[i] = (\text{cipher}[i-1] \cdot \text{block}[i])^e \pmod{N}$

### Solution:

Vậy bây giờ chúng ta phải tìm cách phân tích  $N$  thành  $p, q$   
Sau khi thử với các phương pháp thông thường như factordb.com, RSAtool ... thấy không được, tức là không thể phân tích  $N$  theo cách thông thường.



```
→ RsaCtfTool ./RsaCtfTool.py --createpub --n 11338353891263513280230135468221495787160331263950802093163138819071812348046447334707559242107943238734753876145710104856463092948991985285824825931860793129139080578734054959163984983045730321467579305258509679670238173489881739129842041725214018893774928173649238953654260748398904131800331292288496112021 --e 65537 > key.txt
→ RsaCtfTool ./RsaCtfTool.py --publickey ./key.txt --private
→ RsaCtfTool ./RsaCtfTool.py --publickey ./key.txt --private
```

Lên mạng đọc thấy có lỗi ROCA link. Thử kiểm tra  $N$  có bị lỗi đó hay không,

tạo pub.pem với  $e = 65537$ . Kiểm tra trên link ta thấy key dính lỗi.

## Results

The key is subject to ROCA, which reduces the security below generally acceptable level.

|                       |  |
|-----------------------|--|
| Type / Interpretation | RSA key                                  |
| Bit length            | 1024                                     |
| Test result           | Subject to ROCA vulnerability, insecure. |

Tìm loang quanh trên mạng thấy có một số tool để tấn công. Một là nekasong tool này chỉ hỗ trợ 512 bit. Hai là udan11. Ném N vào tool này và chạy trên công cụ sagemath thấy phân tích được. Đến đây thì ngon rồi!

```
pvqu47@ubuntu: /mnt/hgfs/D/roca-master
File Edit View Search Terminal Help
* M = 7.24576134690965e65
* X <= M
-> GOOD

# Solutions possible?

we can find a solution if  $2^{((n-1)/4)} * \det(L)^{(1/n)} < N^{(\beta * m)} / \sqrt{n}$ 
*  $2^{((n-1)/4)} * \det(L)^{(1/n)} = 2.73243713251504e579$ 
*  $N^{(\beta * m)} / \sqrt{n} = 1.12767998355292e617$ 
*  $2^{((n-1)/4)} * \det(L)^{(1/n)} < N^{(\beta * m)} / \sqrt{n}$ 
-> SOLUTION WILL BE FOUND

# Note that no solutions will be found _for sure_ if you don't respect:
* |root| < X
* b >= modulus^beta

00 X 0 0 0 0 0 0 0 ~
01 X X 0 0 0 0 0
02 X X X 0 0 0 0
03 X X X X 0 0 0
04 X X X X X 0 0
05 0 X X X X 0 0
06 0 0 X X X X 0
07 0 0 0 X X X X X
potential roots: [(421218708934506345774639149858892991198662285836279123965761703075519160379875477712608229643331669985034300487551412086096
10160046300950753652003377723854, 1), (625988793368758805449617440446603265398902960408967183808853, 3), (17620018103460303583988395904492415
167699131382765770479747207232648960319/281474976710656, 3)]

# Solutions
we want to find: 625988793368758805449617440446603265398902960408967183808853
we found: [42121870893450634577463914985889299119866228583627912396576170307551916037987547771260822964333166998503430048755141208609610160046
300950753652003377723854, 625988793368758805449617440446603265398902960408967183808853]
in: 0.0192880630493 seconds
-- Attacking --
(117963953208421088577464949922641635666511467777502217715766620254076829361011661626404406010733731660981272738741343382874412262159251259917
86575302665317, 961171068184759902561665664214679774493526495370679170178220112625919605948795879188980660355355766521009182886657967224227303
548915653235562336722873713)
pvqu47@ubuntu: /mnt/hgfs/D/roca-master$
```

Từ  $e, p, q$  tính được  $r_{new} = e - (p - 1).(q - 1)$   
 $m = c^d \% N$  với  $d = r_{new}^{-1} \bmod lcm(p - 1, q - 1)$   
Đến đây lần lượt giải từng block để thu được Flag.