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 $e = rnew + (p-1) \cdot (q-1)$

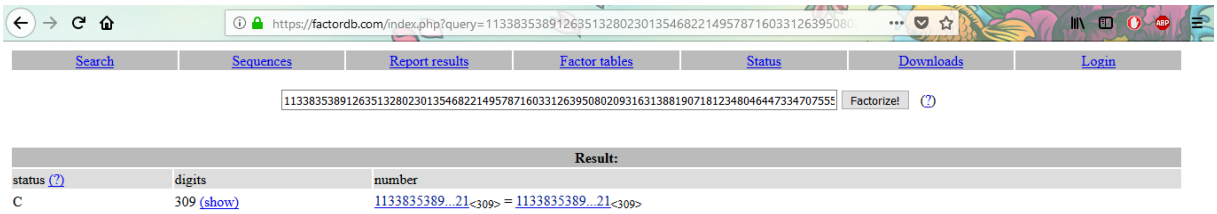
Theo Định lý Fermat có $m^{p-1} \equiv 1(\mod p), m^{q-1} \equiv 1(\mod q) \rightarrow m^{(p-1)(q-1)} \equiv 1(\mod N) \rightarrow c = m^{rnew} \% N$. Do vậy hàm transform sẽ không có ý nghĩa gì nữa. Thuật toán mã hóa sẽ như sau:

Mã hóa:

cipher[0] = (block[0]) ^{e} mod N
cipher[1] = (cipher[0][:size*2+1]) + block[1]) ^{e} mod N
...
cipher[i] = (cipher[i-1][:size*2+1] + block[i]) ^{e} mod 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 113383538912635132802301354682214957871603312639508020931631388190718123480464473347075559242107943238734753876145710104856463092948991985285824825931860793129139080578734054959163984983045730321467579305258509679670238173489881739129842041725214018893774928173649238953654260748398904131800331292288496112021 --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,

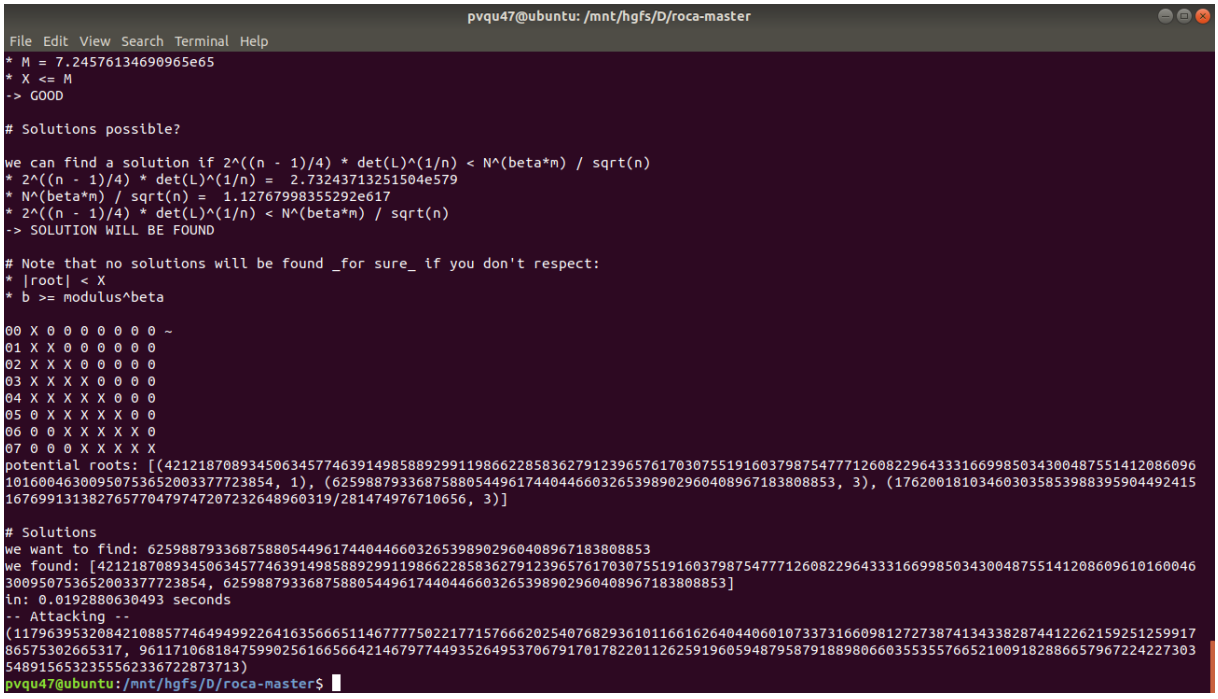
tạo pub.pem với e = 65537. Kiểm tra trên link ta thấy key dính lỗi.

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 loanh quanh trên mạng thấy có một số tool để tấn công. Một là neca song 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!



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