BUUCTF Crypto RSA4

原创

qtL0ng 于 2020-06-06 16:50:04 发布 882 收藏 4

分类专栏： Crypto-RSA

本文链接：https://blog.csdn.net/jianpanliu/article/details/106588963

低加密指数广播攻击

题目如下：

```
N = 331310324212000030020214312244232222400142410423413104441140203003243002104333214202031202212403400220031202
142322434104143104244241214204444443323000244130122022422310201104411044030113302323014101331214303223312402430402
024044130332431321010104222401331222114004340232222142314024034032000122210233413333400423431223021134102101102212
123324130302443133000130340402010444244312013000033411004243201020340144040401000344200122304221144200141300 4
c = 310020004234033042442004214144133203413010021230303112023402224103014234403124124402402441102001121411402012
240324022321312042130123032044220033000040114341021413212233112432420100141404224113423043222012411124021322031 0
113122122300402200312000211023002334114320140431134031113423014023141220133333314240242313433321130210241311111 1
424430032440123340034044314223400401224111323000242234420441240411021023100222003123214343030122032301042243

N = 302240000040421410144422133334143140011011044322223144412002220243001141141114123223331331304421113021231204
322233120121444434210041232214144413244434424302311222143224402302432102242132244032010020113224011210432321432
212034242431340443140222120243431000423420024323311443002142124140334141200043442113302240203012230333343242440 3
120424012230124223201130321122004422241113440301213242031111030244234402112210122441123000220334414014304411 4
c = 112200203404013430330214124004404423210041321043000303233141423344144222343401042200334033203124030011440014 2
101121032344403121340321234004443441442330201301101340421022203020024133211020224141304430411442403101210201003 1
010433420423441241142442032121111223203112133031033341442343334332202440012120033333043222342143334412202301244 0
013041401423022101240244310400134143131211234334241131134144220433304220023141441111341420443334041122403 44

N = 332200324410041111434222123043121331442103233332422341041340412034230003314420311333101344231212130200312041
044324431141033004333110021013020140020011222012300020041342040004002220210223122111314112124333211132230332124 0
224231412140313031444441344030244201114232444240300300033402130321213032133430204013042433300013140230301210341 1
333440444042124224011310320301334123133000433204030244001132400413032403432343014310240144013024232142402032 3
c = 100134441201411303224433204124002242224332334011124210012440241402342100410331131441303242011002101323040403311
120421304422222200324402244243322422444414043342130111111330022213203030324422101133032212042042243101434342203
204121042113212104212423330331134311311111414320001124000211131212223434000340331204040104302143311203133432432213
233041123400140301320214321011302112411344224134423120130421412120031022113003214040430121243320132404312 42
```

关于低加密指数广播攻击：

> 如果选取的加密指数较低，并且使用了相同的加密指数给一个接受者的群发送相同的信息，那么可以进行广播攻击得到明文。
> 即，选取了相同的加密指数e（这里取e=3），对相同的明文m进行了加密并进行了消息的传递，那么有：

识别：

> 一般来说都是给了三组加密的参数和明密文，其中题目很明确地能告诉你这三组的明文都是一样的，并且e都取了一个较小的数字。

对以上c的求解可通过中国剩余定理

另外有两点需要注意：

1、此题中的N、c均是以5进制表示，要先用int("******",5)转换为十进制才能计算(开始运行半天都不出结果，看了其他师傅博客才发现原来是五进制)。

2、题目没有给出加密指数e，但是根据低加密指数广播攻击的特性猜e=3、10、17等

解题脚本：

```
# -*- coding: UTF-8 -*-
import gmpy2
import libnum

def CRT(data):
 sum = 0
 m = 1
 for n in data:
  m = m*n[0]
 for n,c in data:
  m1 = m/n
  mr = gmpy2.invert(m1,n)
  sum = sum+mr*m1*c
 return sum%m

N1 = int('331310324212000030020214312244232222400142410423413104441140203003243002104333214202031202212403400220031
202142322434104143104244241214204444443323000244130122022422310201104411044030113302323014101331214303223312402 4
304024044130332431321010104222401331222114004340232222142314024034032000122210233413333400423431223021134102101 1
022123324130302443133000130340402010444244312013000033411004243201020340144040401000344200122304221144200141300 4
',5)
c1 = int('310020004234033304244200421414413320341301002123030311202340222410301423440312412440240244110200112141140
201224032402232131204213012303204422003300004011434102141321223311243242010014140422411342304322201241112402132 2
031011312212230040220031200021102300233411432014043113403111342301402314122013333331424024231343332113021024131 1
111142443003244012334003404431422340040122411132300024223442044124041102102310022200312321434303012203230104224 3
',5)
N2 = int('302240000040421410144422133334143140011011044322223144412002220243001141141114123223331331304421113021231
204322233120121444434210041232214144413244434424302311222143224402302432102242132244032010020113224011121043232 1
432212034242431340443140222120243431000423420024323311443002142124140334141200043442113302240203012230333343242 4
403120424012230124223201130321122004422241113440301213242031111030244234402112210122441123000220334414014304411 4
',5)
c2 = int('112200203404013430330214124004404423210041321043000303233141423344144222343401042200334033203124030011440
014210112103234440312134032123400444344144233020130110134042102220302002413321102022414130443041144240310121020 1
003101043342042344124114244203212111122320311213303103334144234333433220244001212003333304322234214333441220230 1
244001304140142320221012402443104001341431312112343342411311341442204333042200231414411113414204433340411224034 4
',5)
N3 = int('332200324410041111434222123043121331442103233332422341041340412034230003314420311333101344231212130200312
041044324431141033004333110021013020140020011222012300020041342040004002220210223122111314112124333211132230332 1
240224231412140313031444441344030244201114232444240300300033402130321213032133430204013042433300013140230301210 3
411333440444042124224011310320301334123133000433204030244001132400413032403432343014310240144013024232142402032 3
',5)
c3 = int('100134441201411303224332041240022422243323340111242100124402414023421004103311314413032420110021013230404
033111204213044222220032440224424332242244441404334213011111133002221320303032442210113303221204204224310143434 2
220320412104211321210421242333033113431131111414320001124000211131212223434000340331204040104302143311203133432 4
322123304112340014030132021432101130211241134422413442312013042141212003102211300321404043012124332013240431242',
5)
e = 3

n = [N1,N2,N3]
c = [c1,c2,c3]
data = zip(n,c)
m_e = CRT(data)
m = gmpy2.iroot(m_e,e)[0]
print libnum.n2s(m)
```