CTF-CRYPTO-RSA Polynomial

原创

大熊何在 于 2020-11-17 10:58:19 发布

分类专栏： CRYPTO

本文链接：https://blog.csdn.net/zippo1234/article/details/109738220

CTF-CRYPTO-RSA Polynomial

每天一题，只能多不能少

RSA Polynomial

题目分析

1. polynomial多项式
2. 基于多项式的RSA算法

开始

1.题目

encrypt.sage

```
pri = 31337
R.<x> = PolynomialRing(GF(pri))

def gen_irreducable_poly(deg):
    while True:
        out = R.random_element(degree=deg)
        if out.is_irreducible():
            return out

P = gen_irreducable_poly(ZZ.random_element(2^6, 2^7))
Q = gen_irreducable_poly(ZZ.random_element(2^6, 2^7))

N = P * Q

S.<x> = R.quotient(N)

e = 65537
flag = bytearray(raw_input())
flag = list(flag)
M = S(flag)
C = M ^ e

print 'pri = ' + str(pri)
print 'N = ' + str(N)
print 'C = ' + str(C)
```

output.txt

```
pri = 31337
N = 5788*x^215 + 26497*x^214 + 2006*x^213 + 4161*x^212 + 13803*x^211 + 16883*x^210 + 28928*x^209 + 12337*x^208 +
 23340*x^207 + 15458*x^206 + 2164*x^205 + 17989*x^204 + 11778*x^203 + 7461*x^202 + 3912*x^201 + 12509*x^200 + 25
24*x^199 + 17616*x^198 + 10091*x^197 + 8569*x^196 + 12782*x^195 + 30175*x^194 + 15865*x^193 + 1589*x^192 + 19001
*x^191 + 10057*x^190 + 2125*x^189 + 23649*x^188 + 10083*x^187 + 7914*x^186 + 30250*x^185 + 21636*x^184 + 6021*x^
183 + 12793*x^182 + 16451*x^181 + 14377*x^180 + 29693*x^179 + 8888*x^178 + 7876*x^177 + 19492*x^176 + 3704*x^175
 + 13867*x^174 + 28433*x^173 + 4389*x^172 + 28314*x^171 + 21292*x^170 + 16903*x^169 + 8629*x^168 + 15699*x^167 +
 26700*x^166 + 3556*x^165 + 31294*x^164 + 10491*x^163 + 9922*x^162 + 11278*x^161 + 18600*x^160 + 28135*x^159 + 2
1201*x^158 + 5835*x^157 + 29179*x^156 + 25120*x^155 + 6196*x^154 + 2909*x^153 + 16005*x^152 + 24607*x^151 + 5010
*x^150 + 30228*x^149 + 8295*x^148 + 14039*x^147 + 21119*x^146 + 12261*x^145 + 544*x^144 + 21577*x^143 + 771*x^14
2 + 5324*x^141 + 22125*x^140 + 7449*x^139 + 4975*x^138 + 11478*x^137 + 26395*x^136 + 789*x^135 + 9166*x^134 + 17
953*x^133 + 11420*x^132 + 11758*x^131 + 5734*x^130 + 1042*x^129 + 1914*x^128 + 23356*x^127 + 31040*x^126 + 21915
*x^125 + 13038*x^124 + 25713*x^123 + 19219*x^122 + 16519*x^121 + 24862*x^120 + 23870*x^119 + 22051*x^118 + 27324
*x^117 + 5476*x^116 + 12805*x^115 + 18999*x^114 + 27399*x^113 + 31291*x^112 + 28163*x^111 + 14023*x^110 + 20008*
x^109 + 13034*x^108 + 26496*x^107 + 13766*x^106 + 24315*x^105 + 6977*x^104 + 22992*x^103 + 11873*x^102 + 8177*x^
101 + 15918*x^100 + 22003*x^99 + 16240*x^98 + 15974*x^97 + 23722*x^96 + 17651*x^95 + 4930*x^94 + 6183*x^93 + 286
55*x^92 + 9660*x^91 + 712*x^90 + 10119*x^89 + 19125*x^88 + 30686*x^87 + 18453*x^86 + 15385*x^85 + 19550*x^84 + 1
9519*x^83 + 11300*x^82 + 28406*x^81 + 10650*x^80 + 20720*x^79 + 19026*x^78 + 13302*x^77 + 22456*x^76 + 8222*x^75
 + 13900*x^74 + 12225*x^73 + 5425*x^72 + 30405*x^71 + 26164*x^70 + 1396*x^69 + 11283*x^68 + 16263*x^67 + 19134*x
^66 + 31279*x^65 + 16877*x^64 + 24996*x^63 + 16710*x^62 + 14715*x^61 + 23075*x^60 + 11418*x^59 + 29173*x^58 + 16
289*x^57 + 28046*x^56 + 17240*x^55 + 11415*x^54 + 28414*x^53 + 18835*x^52 + 30971*x^51 + 854*x^50 + 18588*x^49 +
 19558*x^48 + 22203*x^47 + 1991*x^46 + 17138*x^45 + 22804*x^44 + 29858*x^43 + 17180*x^42 + 14530*x^41 + 12799*x^
40 + 29676*x^39 + 629*x^38 + 19090*x^37 + 587*x^36 + 21538*x^35 + 21619*x^34 + 19779*x^33 + 4584*x^32 + 22371*x^
31 + 19408*x^30 + 16879*x^29 + 11100*x^28 + 7338*x^27 + 4729*x^26 + 6507*x^25 + 7434*x^24 + 3959*x^23 + 17913*x^
22 + 10177*x^21 + 2399*x^20 + 7864*x^19 + 6825*x^18 + 14680*x^17 + 28609*x^16 + 22079*x^15 + 5346*x^14 + 24802*x
^13 + 17107*x^12 + 4086*x^11 + 4546*x^10 + 3251*x^9 + 7759*x^8 + 12351*x^7 + 7579*x^6 + 14962*x^5 + 13915*x^4 +
23812*x^3 + 27689*x^2 + 22533*x + 721
C = 3346*x^214 + 29774*x^213 + 13276*x^212 + 28577*x^211 + 14816*x^210 + 9857*x^209 + 5125*x^208 + 3171*x^207 +
8203*x^206 + 5248*x^205 + 22500*x^204 + 1974*x^203 + 21252*x^202 + 15733*x^201 + 7257*x^200 + 12616*x^199 + 9375
*x^198 + 15468*x^197 + 22377*x^196 + 2111*x^195 + 6825*x^194 + 8889*x^193 + 28282*x^192 + 4619*x^191 + 16049*x^1
90 + 3101*x^189 + 20421*x^188 + 17495*x^187 + 25057*x^186 + 1867*x^185 + 16614*x^184 + 18334*x^183 + 1460*x^182
+ 16056*x^181 + 21600*x^180 + 21322*x^179 + 8765*x^178 + 20677*x^177 + 13539*x^176 + 27956*x^175 + 3595*x^174 +
12037*x^173 + 16002*x^172 + 23491*x^171 + 9485*x^170 + 9432*x^169 + 19182*x^168 + 1752*x^167 + 14167*x^166 + 104
39*x^165 + 26946*x^164 + 14661*x^163 + 22742*x^162 + 6173*x^161 + 3480*x^160 + 7223*x^159 + 30598*x^158 + 12953*
x^157 + 4663*x^156 + 10054*x^155 + 22717*x^154 + 1401*x^153 + 16241*x^152 + 4639*x^151 + 44*x^150 + 18134*x^149
+ 6229*x^148 + 24271*x^147 + 7393*x^146 + 7116*x^145 + 302*x^144 + 29235*x^143 + 7286*x^142 + 11039*x^141 + 5128
*x^140 + 23054*x^139 + 3312*x^138 + 22753*x^137 + 13186*x^136 + 15405*x^135 + 23785*x^134 + 15821*x^133 + 21892*
x^132 + 30580*x^131 + 22964*x^130 + 5088*x^129 + 6320*x^128 + 31224*x^127 + 30982*x^126 + 14333*x^125 + 15173*x^
124 + 14104*x^123 + 2816*x^122 + 3799*x^121 + 8284*x^120 + 4522*x^119 + 4759*x^118 + 2259*x^117 + 28111*x^116 +
5537*x^115 + 22532*x^114 + 12465*x^113 + 20770*x^112 + 17069*x^111 + 19026*x^110 + 27833*x^109 + 14411*x^108 + 1
7229*x^107 + 31182*x^106 + 2967*x^105 + 1186*x^104 + 22261*x^103 + 9090*x^102 + 28062*x^101 + 5075*x^100 + 557*x
^99 + 6805*x^98 + 30665*x^97 + 15129*x^96 + 27966*x^95 + 14432*x^94 + 4044*x^93 + 2937*x^92 + 11460*x^91 + 5820*
x^90 + 28014*x^89 + 2374*x^88 + 28649*x^87 + 10864*x^86 + 693*x^85 + 28858*x^84 + 22944*x^83 + 3682*x^82 + 17650
*x^81 + 11532*x^80 + 13225*x^79 + 15240*x^78 + 27253*x^77 + 9633*x^76 + 25244*x^75 + 23993*x^74 + 18491*x^73 + 2
5360*x^72 + 2710*x^71 + 16306*x^70 + 13147*x^69 + 27921*x^68 + 4362*x^67 + 12083*x^66 + 701*x^65 + 23431*x^64 +
29507*x^63 + 9407*x^62 + 19099*x^61 + 30452*x^60 + 13404*x^59 + 26105*x^58 + 8347*x^57 + 21737*x^56 + 7818*x^55
+ 10473*x^54 + 25076*x^53 + 4804*x^52 + 19001*x^51 + 24131*x^50 + 10717*x^49 + 27602*x^48 + 7581*x^47 + 9653*x^4
6 + 26091*x^45 + 14793*x^44 + 13812*x^43 + 28818*x^42 + 8248*x^41 + 12038*x^40 + 27425*x^39 + 12697*x^38 + 6768*
x^37 + 30729*x^36 + 864*x^35 + 5682*x^34 + 7100*x^33 + 1371*x^32 + 15863*x^31 + 31278*x^30 + 16065*x^29 + 14624*
x^28 + 7211*x^27 + 7983*x^26 + 20891*x^25 + 15136*x^24 + 9548*x^23 + 17089*x^22 + 8549*x^21 + 13526*x^20 + 10626
*x^19 + 9576*x^18 + 24733*x^17 + 18300*x^16 + 8682*x^15 + 17996*x^14 + 14781*x^13 + 17305*x^12 + 23365*x^11 + 10
08*x^10 + 2749*x^9 + 20817*x^8 + 7411*x^7 + 4465*x^6 + 7784*x^5 + 27301*x^4 + 14697*x^3 + 27980*x^2 + 25732*x +
19140
```

2.分析

（1）分解N

模数N都可以直接分解成两个多项式的乘积

```
P = 31337
R.<x> = PolynomialRing(GF(P))
N = 5788*x^215 + 26497*x^214 + 2006*x^213 + 4161*x^212 + 13803*x^211 + 16883*x^210 + 28928*x^209 + 12337*x^208 +
 23340*x^207 + 15458*x^206 + 2164*x^205 + 17989*x^204 + 11778*x^203 + 7461*x^202 + 3912*x^201 + 12509*x^200 + 25
24*x^199 + 17616*x^198 + 10091*x^197 + 8569*x^196 + 12782*x^195 + 30175*x^194 + 15865*x^193 + 1589*x^192 + 19001
*x^191 + 10057*x^190 + 2125*x^189 + 23649*x^188 + 10083*x^187 + 7914*x^186 + 30250*x^185 + 21636*x^184 + 6021*x^
183 + 12793*x^182 + 16451*x^181 + 14377*x^180 + 29693*x^179 + 8888*x^178 + 7876*x^177 + 19492*x^176 + 3704*x^175
 + 13867*x^174 + 28433*x^173 + 4389*x^172 + 28314*x^171 + 21292*x^170 + 16903*x^169 + 8629*x^168 + 15699*x^167 +
 26700*x^166 + 3556*x^165 + 31294*x^164 + 10491*x^163 + 9922*x^162 + 11278*x^161 + 18600*x^160 + 28135*x^159 + 2
1201*x^158 + 5835*x^157 + 29179*x^156 + 25120*x^155 + 6196*x^154 + 2909*x^153 + 16005*x^152 + 24607*x^151 + 5010
*x^150 + 30228*x^149 + 8295*x^148 + 14039*x^147 + 21119*x^146 + 12261*x^145 + 544*x^144 + 21577*x^143 + 771*x^14
2 + 5324*x^141 + 22125*x^140 + 7449*x^139 + 4975*x^138 + 11478*x^137 + 26395*x^136 + 789*x^135 + 9166*x^134 + 17
953*x^133 + 11420*x^132 + 11758*x^131 + 5734*x^130 + 1042*x^129 + 1914*x^128 + 23356*x^127 + 31040*x^126 + 21915
*x^125 + 13038*x^124 + 25713*x^123 + 19219*x^122 + 16519*x^121 + 24862*x^120 + 23870*x^119 + 22051*x^118 + 27324
*x^117 + 5476*x^116 + 12805*x^115 + 18999*x^114 + 27399*x^113 + 31291*x^112 + 28163*x^111 + 14023*x^110 + 20008*
x^109 + 13034*x^108 + 26496*x^107 + 13766*x^106 + 24315*x^105 + 6977*x^104 + 22992*x^103 + 11873*x^102 + 8177*x^
101 + 15918*x^100 + 22003*x^99 + 16240*x^98 + 15974*x^97 + 23722*x^96 + 17651*x^95 + 4930*x^94 + 6183*x^93 + 286
55*x^92 + 9660*x^91 + 712*x^90 + 10119*x^89 + 19125*x^88 + 30686*x^87 + 18453*x^86 + 15385*x^85 + 19550*x^84 + 1
9519*x^83 + 11300*x^82 + 28406*x^81 + 10650*x^80 + 20720*x^79 + 19026*x^78 + 13302*x^77 + 22456*x^76 + 8222*x^75
 + 13900*x^74 + 12225*x^73 + 5425*x^72 + 30405*x^71 + 26164*x^70 + 1396*x^69 + 11283*x^68 + 16263*x^67 + 19134*x
^66 + 31279*x^65 + 16877*x^64 + 24996*x^63 + 16710*x^62 + 14715*x^61 + 23075*x^60 + 11418*x^59 + 29173*x^58 + 16
289*x^57 + 28046*x^56 + 17240*x^55 + 11415*x^54 + 28414*x^53 + 18835*x^52 + 30971*x^51 + 854*x^50 + 18588*x^49 +
 19558*x^48 + 22203*x^47 + 1991*x^46 + 17138*x^45 + 22804*x^44 + 29858*x^43 + 17180*x^42 + 14530*x^41 + 12799*x^
40 + 29676*x^39 + 629*x^38 + 19090*x^37 + 587*x^36 + 21538*x^35 + 21619*x^34 + 19779*x^33 + 4584*x^32 + 22371*x^
31 + 19408*x^30 + 16879*x^29 + 11100*x^28 + 7338*x^27 + 4729*x^26 + 6507*x^25 + 7434*x^24 + 3959*x^23 + 17913*x^
22 + 10177*x^21 + 2399*x^20 + 7864*x^19 + 6825*x^18 + 14680*x^17 + 28609*x^16 + 22079*x^15 + 5346*x^14 + 24802*x
^13 + 17107*x^12 + 4086*x^11 + 4546*x^10 + 3251*x^9 + 7759*x^8 + 12351*x^7 + 7579*x^6 + 14962*x^5 + 13915*x^4 +
23812*x^3 + 27689*x^2 + 22533*x + 721
p,q = N.factor()
```

（2）欧拉函数

欧拉函数的定义

```
对于整数n来讲，欧拉函数phi(n)表示所有小于或等于n的正整数中与n互质的数的数目。
对于多项式P(y)来讲，欧拉函数phi(P(y))表示所有不高于P(y)幂级的环内所有多项式中，与P(y)无除1以外的公因式的其他多项式的个数。
```

P(x)和Q(x)是多项式GF§上的，因此这里phi的值应该等于

```
(p**P(x).degree()-1)*(p**Q(x).degree()-1)
```

（3）提取多项式的参数

使用list方法获取多项式的参数，最终的结果中多项式的参数就是flag。

3.上脚本

```
#!python3
# -*- coding: utf-8 -*-
# @Time : 2020/11/17 10:36
# @Author : A.James
# @FileName: tt2.py
from binascii import *

P = 31337
R.<x> = PolynomialRing(GF(P))
N = 5788*x^215 + 26497*x^214 + 2006*x^213 + 4161*x^212 + 13803*x^211 + 16883*x^210 + 28928*x^209 + 12337*x^208 +
 23340*x^207 + 15458*x^206 + 2164*x^205 + 17989*x^204 + 11778*x^203 + 7461*x^202 + 3912*x^201 + 12509*x^200 + 25
24*x^199 + 17616*x^198 + 10091*x^197 + 8569*x^196 + 12782*x^195 + 30175*x^194 + 15865*x^193 + 1589*x^192 + 19001
*x^191 + 10057*x^190 + 2125*x^189 + 23649*x^188 + 10083*x^187 + 7914*x^186 + 30250*x^185 + 21636*x^184 + 6021*x^
```

```
183 + 12793*x^182 + 16451*x^181 + 14377*x^180 + 29693*x^179 + 8888*x^178 + 7876*x^177 + 19492*x^176 + 3704*x^175
 + 13867*x^174 + 28433*x^173 + 4389*x^172 + 28314*x^171 + 21292*x^170 + 16903*x^169 + 8629*x^168 + 15699*x^167 +
 26700*x^166 + 3556*x^165 + 31294*x^164 + 10491*x^163 + 9922*x^162 + 11278*x^161 + 18600*x^160 + 28135*x^159 + 2
1201*x^158 + 5835*x^157 + 29179*x^156 + 25120*x^155 + 6196*x^154 + 2909*x^153 + 16005*x^152 + 24607*x^151 + 5010
*x^150 + 30228*x^149 + 8295*x^148 + 14039*x^147 + 21119*x^146 + 12261*x^145 + 544*x^144 + 21577*x^143 + 771*x^14
2 + 5324*x^141 + 22125*x^140 + 7449*x^139 + 4975*x^138 + 11478*x^137 + 26395*x^136 + 789*x^135 + 9166*x^134 + 17
953*x^133 + 11420*x^132 + 11758*x^131 + 5734*x^130 + 1042*x^129 + 1914*x^128 + 23356*x^127 + 31040*x^126 + 21915
*x^125 + 13038*x^124 + 25713*x^123 + 19219*x^122 + 16519*x^121 + 24862*x^120 + 23870*x^119 + 22051*x^118 + 27324
*x^117 + 5476*x^116 + 12805*x^115 + 18999*x^114 + 27399*x^113 + 31291*x^112 + 28163*x^111 + 14023*x^110 + 20008*
x^109 + 13034*x^108 + 26496*x^107 + 13766*x^106 + 24315*x^105 + 6977*x^104 + 22992*x^103 + 11873*x^102 + 8177*x^
101 + 15918*x^100 + 22003*x^99 + 16240*x^98 + 15974*x^97 + 23722*x^96 + 17651*x^95 + 4930*x^94 + 6183*x^93 + 286
55*x^92 + 9660*x^91 + 712*x^90 + 10119*x^89 + 19125*x^88 + 30686*x^87 + 18453*x^86 + 15385*x^85 + 19550*x^84 + 1
9519*x^83 + 11300*x^82 + 28406*x^81 + 10650*x^80 + 20720*x^79 + 19026*x^78 + 13302*x^77 + 22456*x^76 + 8222*x^75
 + 13900*x^74 + 12225*x^73 + 5425*x^72 + 30405*x^71 + 26164*x^70 + 1396*x^69 + 11283*x^68 + 16263*x^67 + 19134*x
^66 + 31279*x^65 + 16877*x^64 + 24996*x^63 + 16710*x^62 + 14715*x^61 + 23075*x^60 + 11418*x^59 + 29173*x^58 + 16
289*x^57 + 28046*x^56 + 17240*x^55 + 11415*x^54 + 28414*x^53 + 18835*x^52 + 30971*x^51 + 854*x^50 + 18588*x^49 +
 19558*x^48 + 22203*x^47 + 1991*x^46 + 17138*x^45 + 22804*x^44 + 29858*x^43 + 17180*x^42 + 14530*x^41 + 12799*x^
40 + 29676*x^39 + 629*x^38 + 19090*x^37 + 587*x^36 + 21538*x^35 + 21619*x^34 + 19779*x^33 + 4584*x^32 + 22371*x^
31 + 19408*x^30 + 16879*x^29 + 11100*x^28 + 7338*x^27 + 4729*x^26 + 6507*x^25 + 7434*x^24 + 3959*x^23 + 17913*x^
22 + 10177*x^21 + 2399*x^20 + 7864*x^19 + 6825*x^18 + 14680*x^17 + 28609*x^16 + 22079*x^15 + 5346*x^14 + 24802*x
^13 + 17107*x^12 + 4086*x^11 + 4546*x^10 + 3251*x^9 + 7759*x^8 + 12351*x^7 + 7579*x^6 + 14962*x^5 + 13915*x^4 +
23812*x^3 + 27689*x^2 + 22533*x + 721
S.<x> = R.quotient(N)
C = 3346*x^214 + 29774*x^213 + 13276*x^212 + 28577*x^211 + 14816*x^210 + 9857*x^209 + 5125*x^208 + 3171*x^207 +
8203*x^206 + 5248*x^205 + 22500*x^204 + 1974*x^203 + 21252*x^202 + 15733*x^201 + 7257*x^200 + 12616*x^199 + 9375
*x^198 + 15468*x^197 + 22377*x^196 + 2111*x^195 + 6825*x^194 + 8889*x^193 + 28282*x^192 + 4619*x^191 + 16049*x^1
90 + 3101*x^189 + 20421*x^188 + 17495*x^187 + 25057*x^186 + 1867*x^185 + 16614*x^184 + 18334*x^183 + 1460*x^182
+ 16056*x^181 + 21600*x^180 + 21322*x^179 + 8765*x^178 + 20677*x^177 + 13539*x^176 + 27956*x^175 + 3595*x^174 +
12037*x^173 + 16002*x^172 + 23491*x^171 + 9485*x^170 + 9432*x^169 + 19182*x^168 + 1752*x^167 + 14167*x^166 + 104
39*x^165 + 26946*x^164 + 14661*x^163 + 22742*x^162 + 6173*x^161 + 3480*x^160 + 7223*x^159 + 30598*x^158 + 12953*
x^157 + 4663*x^156 + 10054*x^155 + 22717*x^154 + 1401*x^153 + 16241*x^152 + 4639*x^151 + 44*x^150 + 18134*x^149
+ 6229*x^148 + 24271*x^147 + 7393*x^146 + 7116*x^145 + 302*x^144 + 29235*x^143 + 7286*x^142 + 11039*x^141 + 5128
*x^140 + 23054*x^139 + 3312*x^138 + 22753*x^137 + 13186*x^136 + 15405*x^135 + 23785*x^134 + 15821*x^133 + 21892*
x^132 + 30580*x^131 + 22964*x^130 + 5088*x^129 + 6320*x^128 + 31224*x^127 + 30982*x^126 + 14333*x^125 + 15173*x^
124 + 14104*x^123 + 2816*x^122 + 3799*x^121 + 8284*x^120 + 4522*x^119 + 4759*x^118 + 2259*x^117 + 28111*x^116 +
5537*x^115 + 22532*x^114 + 12465*x^113 + 20770*x^112 + 17069*x^111 + 19026*x^110 + 27833*x^109 + 14411*x^108 + 1
7229*x^107 + 31182*x^106 + 2967*x^105 + 1186*x^104 + 22261*x^103 + 9090*x^102 + 28062*x^101 + 5075*x^100 + 557*x
^99 + 6805*x^98 + 30665*x^97 + 15129*x^96 + 27966*x^95 + 14432*x^94 + 4044*x^93 + 2937*x^92 + 11460*x^91 + 5820*
x^90 + 28014*x^89 + 2374*x^88 + 28649*x^87 + 10864*x^86 + 693*x^85 + 28858*x^84 + 22944*x^83 + 3682*x^82 + 17650
*x^81 + 11532*x^80 + 13225*x^79 + 15240*x^78 + 27253*x^77 + 9633*x^76 + 25244*x^75 + 23993*x^74 + 18491*x^73 + 2
5360*x^72 + 2710*x^71 + 16306*x^70 + 13147*x^69 + 27921*x^68 + 4362*x^67 + 12083*x^66 + 701*x^65 + 23431*x^64 +
29507*x^63 + 9407*x^62 + 19099*x^61 + 30452*x^60 + 13404*x^59 + 26105*x^58 + 8347*x^57 + 21737*x^56 + 7818*x^55
+ 10473*x^54 + 25076*x^53 + 4804*x^52 + 19001*x^51 + 24131*x^50 + 10717*x^49 + 27602*x^48 + 7581*x^47 + 9653*x^4
6 + 26091*x^45 + 14793*x^44 + 13812*x^43 + 28818*x^42 + 8248*x^41 + 12038*x^40 + 27425*x^39 + 12697*x^38 + 6768*
x^37 + 30729*x^36 + 864*x^35 + 5682*x^34 + 7100*x^33 + 1371*x^32 + 15863*x^31 + 31278*x^30 + 16065*x^29 + 14624*
x^28 + 7211*x^27 + 7983*x^26 + 20891*x^25 + 15136*x^24 + 9548*x^23 + 17089*x^22 + 8549*x^21 + 13526*x^20 + 10626
*x^19 + 9576*x^18 + 24733*x^17 + 18300*x^16 + 8682*x^15 + 17996*x^14 + 14781*x^13 + 17305*x^12 + 23365*x^11 + 10
08*x^10 + 2749*x^9 + 20817*x^8 + 7411*x^7 + 4465*x^6 + 7784*x^5 + 27301*x^4 + 14697*x^3 + 27980*x^2 + 25732*x +
19140

p,q = N.factor()
p,q = p[0],q[0]
s = (P**p.degree()-1)*(P**q.degree()-1)
#print s
e = 65537
d = inverse_mod(e,s)
M = C^d
#print M
#print M.list()
```

```
print ("".join([chr(c) for c in M.list()]))
```

4.get flag

```
flag{RSA_in_polynomial_ring_seems_hard}
```

结语

多项式RSA