MATH 3H03 - RSA WORKSHEET (LECTURE 27)

In our last lecture, we were introduced to the RSA algorithm. Below, I have encoded a passage from a book using the RSA algorithm. You goal is to break the code, and answer the question:

What university did the author of the book attend?

Working in groups up to four people, you may use any resource available to you.

Here's how the encoding was done. Suppose we wanted to encode

Number theory is the best.

Each letter is turned into the corresponding number from 01 to 26. In particular, the above sentence is turned into:

142113020518200805151825091920080502051920

All spaces and punctuation have been eliminated. The number was then broken into blocks of size 12 (or smaller):

142113020518 200805151825 091920080502 051920

Using the public key (n, e) where $n = 2,500,494,517,667$ and $e = 619,590,694,577$, for each block m above, we compute $m^e \pmod{n}$ to get:

1238763098216 200805151825 1292171821964 79446577063

The blocks given below have all been coded using this public key (n, e).

[**HINT:** When you decode each block, you should get a 12 digit number. If you only get 11 digits, you need to add a 0 to the beginning of the digit. Each block will give you 6 letters of the message.]

Encrypted passage

1732446945885
956597824544
328858297167
668584311716
1345574229737
986869093029
126219351014
893970229956
175784202750
1144045233149

1064299682023
121972131206
1197138511811
75990782137
2236599539970
42686918827
1273078573314
1059844108694

224692641483
64622084259

808432919406
1547745093729
2436653995000
1088220978240
1567193566027
2174046861502
1947308588725
578259344781
459272533073
1827241429219

1328757590810
1273078573314
2236600977505
1158937861874
2272408073704
2152941756194
1238763098216
1183252699188
837622808551
98416164349

2219192648011
2348114338881
2207137416625
1547320954239
1286057004599
2265224908240

(Solution)

Here is one way to approach this using Sage commands:

```
# enter public key
n = 2500494517667
e = 619590694577

# factor the n
factor(n)

# out put is 1000151 * 2500117

# determine the two primes
p= 1000151
q= 2500117

# determine phin
phin = (p-1)*(q-1)

## solve e*x = 1 mod phin to get the decoding key
solve_mod(e*x == 1,phin)

### the decoding key (the output of the last command)
f = 113

## input coded list
L = [1732446945885,
956597824544,
328858297167,
668584311716,
1345574229737,
986869093029,
126219351014,
893970229956,
175784202750,
1144045233149,
1064299682023,
121972131206,
1197138511811,
75990782137,
2236599539970,
42686918827,
1273078573314,
1059844108694,
224692641483,
64622084259,
808432919406,
1547745093729,
2436653995000,
1088220978240,
1567193566027,
```

```
2174046861502,
1947308588725,
578259344781,
459272533073,
1827241429219,
1328757590810,
1273078573314,
2236600977505,
1158937861874,
2272408073704,
2152941756194,
1238763098216,
1183252699188,
837622808551,
98416164349,
2219192648011,
2348114338881,
2207137416625,
1547320954239,
1286057004599,
2265224908240]

###

Decode = []
for i in range(len(L)):
   b = L[i]^f % n
   Decode.append(b)

Decode
```

The output of the last command then gives you the strings:

```
230805140904,
 51903051404,
 50408051805,
 91901232515,
 211806152118,
 191514192008,
 51605142001,
 71514190501,
 30809140809,
 190116011820,
 130514200114,
 42515211820,
 231507180114,
 41915141920,
 80508052401,
 71514190919,
 12325152118,
 251521140705,
 192008052401,
```

```
71514180513,
10914012308,
91205230920,
82515210114,
42008051418,
52009180520,
150809191815,
151312050122,
91407251521,
11404251521,
182309060501,
121514050919,
12325152118,
91915190305,
120519190518,
220114201920,
81805050914,
142113020518,
91420080511,
92003080514,
12019211616,
51801140420,
80512092020,
120516010705,
91420080519,
32112120518,
25]
```

We now use the the website

`http://rumkin.com/tools/cipher/numbers.php`

(you have to be careful, since the above list is missing the leading zeroes!) If you do everything correctly, you should be able to get:

> *When I descended here, I saw your four Sons, the Pentagons, each in his apartment, and your two Grandsons the Hexagons; I saw your youngest Hexagon remain a while with you and then retire to his room, leaving you and your Wife alone. I saw your Isosceles servants, three in number, in the kitchen at supper, and the little Page in the scullery.*

A quick search on Google will reveal that this passage is taken from *Flatland* by Edwin Abbott Abbott. Then Wikipedia will tell you that he want to **St. John's College, Cambridge**, which is the desired answer.