Homework #2

Due date: 20/10/2017
Notes:

- Computer programs and other soft material must be submitted through sucourse.
- Winzip your programs and add a readme.txt document to explain the programs and how to use them.
- Name your winzip file as "cs411_507_hw02_yourname.zip"

1. (**20 pts**) Consider the following modulus:

n=93923989829536838645425792878391884185852090015047096928325495680735077974573254200941142654635659889069058397106827931666572379715390977199861730622956934976456672365327932404671265952251676873946441183498231232238528978514016592480741429133646590466736838628474537927484115146306435052269979805285188280829

Consider also the following number:

y=56944778095026064508803320557324194828217604358002584860993983127246257172572625621288924208876440674553832158479040031724187898214806257072823966168352349606611537362177018477860328420295741255602485512749523176875861988864327723267007959112818744831884377494800464304976689851182957989115066715277845807162

The integer y is a quadratic residue modulus n, and its square roots are known:

{
11539293044780349664317193739835099161008802876501927386196632728052884864570713532203427639431106901813684612368583348366278480903942058202903897004649103055743285751895970690426609694759832511976035062765586527404034628524567695175048634551582051994897593554954834163440853023500476963332472457537871514030,

65462078929074573896561682473134429960343753900612807859205872292206976673766764795638688642515250572910065281537469802520465145301193070320295080324024966677495122426689606204830245523869232443939539387029183651868429281477875679397889633306037656227303018935833418527282673149878942564121394686954099450002,

284619109004622647488641104052574542255083361144342890691196233885281013008064894053024540121204093161589931155693581291461072344141979068795666502989319682989615499386383261998410204283824444300069017964690475803

70099697036140913082851795827608934239433819692641119400201441996427492488148585118331088830827,

82384696784756488981108599138556785024843287138545169542128862952682193110002540668737715015204552987255373784738244583300293898811448918996957833618307831920713386613431961714244656257491844361970406120732644704834494349989448897305692794582064538471839245073519703764043262122805958088937507347747316766799

}

Factor n.

2. (**20 pts**) Consider the group Z_{46}^{*}.

   a. How many elements are there in the group Z_{46}^{*}? List the elements of Z_{46}^{*}. (**5 pts**)

   b. Find all the generators in the group Z_{46}^{*}. (**5 pts**)

   c. How many elements are there in the group Q_{46}^{*}? The group Q_{46}^{*} consists of all residues in Z_{46}^{*}, which are relatively prime to 46. List the elements of Q_{46}^{*}. (**5 pts**)

   d. Find the generators in Q_{46}^{*}. (**5 pts**)

3. (**30 pts**) Consider the following numbers:

   p=
   12997110888321186459316436989724265349460712629389513072528028592113499927549315535209275673470089822303733552137264381101263928058260190003283395786606613

   q=
   12208677561088985820124024567796306546470708824672729385334541873189398794633650052335324309711480763919028490727764288604694220087933148985261608483250761

   n=p×q

   m=
   104508383527831908823036869386648261753406819764116432937577039021334848453871469297253914394880121355608067237189088530241064709118310089323613713098921642285063603825756456138538154719968501891170428872546150841926912027053577225264111903314505091217903294998448178692295392732881494063202944747727969714684

   e = 67

a. Compute $c \equiv m^e \bmod n$ (Hint: you can use `pow(m, e, n)` function of Python) . (**5 pts**)

b. Compute the number d such that $e \times d \equiv 1 \bmod \phi(n)$, compute $m' \equiv c^d \bmod n$, and show that $m = m'$. (**5 pts**)

c. Compute $c^d \bmod n$ using Chinese Remainder theorem and p and q. You are allowed to perform exponentiation operation only in mod p and mod q. List also the following values: $c_p = c \bmod p$, $c_q = c \bmod q$, $d_p = d \bmod (p-1)$, $d_q = d \bmod (q-1)$, $p^{-1} \bmod q$, $q^{-1} \bmod p$, $c_p^{d_p} \bmod p$, and $c_q^{d_q} \bmod q$. (**15 pts**)

d. Measure the execution times of the exponentiation methods in (b) and (c) using the Python function as follows:

```
import timeit
import time

…

iter = 100
t1 = time.clock()
for i in range(0, iter):
    pow(c, d, n)
t2 = time.clock()
print t2-t1
```

Which one is faster? (<u>Warning</u>: In exponentiation with CRT, you should not include the execution times of values that can be precomputed, such as $p^{-1} \bmod q$ and $q^{-1} \bmod p$)

4. (**15 pts**) Solve the following equations of the form $ax \equiv b \bmod n$ and find all solutions for x if a solution exists. In case there is no solution, your answer must be "NO SOLUTION", and explain why there is no solution.

a. n = 1200320707477907914300088049880
   a = 721194153583451709622550081 7
   b = 1020922994252285219721495971 63 (**5 pts**)

b. n = 120032070747790791430008804988
   a = 445756931670435019004491091 90
   b = 846640782842050683145145800 89 (**5 pts**)

c. n = 120032070747790791430008804988
   a = 404
   b = 212488438968024653019808098 2220 (**5 pts**)

5. (**15 pts**) Consider the following two polynomials over GF(2) :

   $p_1(x) = x^6 + x + 1$
   $p_2(x) = x^6 + x^2 + 1$

   a. Are they irreducible over GF(2)? Explain your answer. (**5 pts**)

   b. Are they primitive over GF(2)? You need to show whether the roots of these polynomials generate all nonzero elements of the field GF(2^6) which has 64 elements. (**10 pts**)