**Homework #2**

Due date: 24/10/2018

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=7519197963616825059473475919665272935688024085617838056506345489899068679826922644904433165878890900819649430009054548164262464489216932204311933941987267253245684421002477067674284279907689858948515642332083283659312231907446846847748777699985285177717295366767158551808673171192059742572047913270325915613

Consider also the following number:

y=3209914600874008500669935401430665363662412488153089828835443261030801437200212347910860119033606488561197004601674106596598459681203418060565894194568759290922801528229679761127331866325136546667744322264558258342327040988162854318186593925780283235229957993222433235872039468178675216535512488042635755042

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

{ 3708938308454104516702151825577264734932704619196334493742102012085049133860066916102730058438177755140779946753156246803295551884416938289763313330523905172072027042248481556236130811168223100218388139803554641018491672049531817488615769186936860939150325755164461297959399070505580168312640786987386537970,

3810259655162720542771324094088008200755319466421503562764243477814019545966855728801703107440713145678869483255898301360966912604799993914548620611463362081173657378753995511438153468739466758730127502528528642640820559857915029359133008513048424238566969611602697253849274100686479574259407126282939377643,

1204281249197785714266442632825140385815760158008253320866738851601057451123077855202576520382301531140434905065394058045630903820174243044223260732733986914562762640400496995411532307823305824643456122585957628552765307683540837887390010934716580867984045247189957418104618386361581534738350103893735668456,

6314916714419039345207033286840132549872263927609584735639606638298011228703844789701856645496589369679214524943660490118631560669042689160088673209253280338682921780601980072262751972084384034305059519746125655106546924223906008960358766765268704309733250119577201133704054784830478207833697809376590247157

}

Factor n.

1. (**20 pts**) Consider the group .
   1. How many elements are there in the group ? List the elements of . (**5 pts**)
   2. Find all the generators in the group . (**5 pts**)
   3. How many elements are there in the group ? The group consists of all residues in , which are relatively prime to 58. List the elements of . (**5 pts**)
   4. Find the generators in . (**5 pts**)
2. (**30 pts**) Consider the following numbers:

p= 10106404377238244429826597333701722135807526565404559030730896339579442857374388664504194768519009799965064145557030402164596983123568189834021494235031749

q= 13163502274590772696691357017188157383494073914454743555560229941893711785933411409679348168803213122008986323048364979277888128708485862429032314868646957

n=p×q

c= 86558429746256786220797160070602630299194622171442102432718868178774008203963283371082296312613592328933331443800737112868177768290770644915753506516969943009267919574620060086036513229518287908509845029476546407334692827450859273444583008387805272482776780230890488254799112954960574416568539455497347050126

e = 67

1. (**10 pts**) Compute m = cd mod n (where d = e-1 mod φ(n)).
2. (**10 pts**) Compute cd mod n using Chinese Remainder theorem and p and q. You are allowed to perform exponentiation operation only in mod p and mod q. List the following values: cp = c mod p, cq = c mod q, dp = d mod (p-1), dq = d mod(q-1), p-1 mod q, q-1 mod p, cpdp mod p, and cqdq mod q.
3. (**10 pts**) Measure the execution times of the exponentiation methods in (a) and (b) 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? (Warning: In exponentiation with CRT, you should not include the execution times of values that can be precomputed, such as p-1 mod q and q-1 mod p

1. (**20 pts**) Solve the following equations of the form ax ≡ b mod 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.
   1. n = 876757185537497549441688380876

a = 726529482843138430251706107365

b = 374479581720142608093094131318

* 1. n = 876757185537497549441688380876

a = 682523910410036363063715440006

b = 233807680780339430865969182340

* 1. n = 876757185537497549441688380876

a = 217662435485891894157847112298

b = 815512939769276810314824385915s

1. (**10 pts**) Consider the following binary connections polynomials for LFSR :

p1(x) = x5 + x + 1

p2(x) = x4 + x3 + 1

Do they generate maximum period sequence?