CIS 3362 Homework #5
Number Theory, RSA
Check WebCourses for the due date
Please work in pairs and put both people's names on each file submitted!

1) Write a program that prompts the user to enter an integer, n, in between 1 and 10^{12} and calculates φ(n).

2) Using your program from question 1, write a program that determines if (a) an input value in between 1 and 10^{12} is prime, and (b) if so, asks the user to enter an integer in between 1 and the prime number minus 1 and determines if that value is a primitive root. Your program should work as follows:

Calculate each unique prime factor q_i of p – 1, and calculate $x^{(p-1)/q_i}$ mod p for each q_i. If none of these are equal to 1, then x is a primitive root.

3) A primitive root, α, of a prime, p, is a value such that when you calculate the remainders of α, α^2, α^3, α^4 , ... , α^{p-1}, when divided by p, each number from the set {1, 2, 3, ..., p-1} shows up exactly once. Prove that a prime p has exactly φ(p-1) primitive roots. In writing your proof, you may assume that at least one primitive root of p exists. (Normally, this is the first part of the proof.) (Note: This question is difficult, so don't feel bad if you can't figure it out.)

4) Alice and Bob are using Diffie-Hellman to exchange a secret key. They are using the prime number p = 1234577 and the generator g = 1225529. Alice picks a secret value a and sends g^a = 654127 to Bob. Bob picks a secret value b and sends g^b = 221505 to Alice. What is the secret key they share?

5) Decrypt the following message:

204298354508286797413 50
260227996268125919805 67
305721142249215613443 99
141804248336734145620 55
195392829833936761423 12

These 5 blocks of cipher text were created with a set of RSA public keys that follow:

n = 43767782750765499923141
e = 986321785648512635467

When you decrypt, you'll initially get numbers, but those numbers can be converted into blocks of 16 letters each.