CIS 3362 Homework #6
Number Theory, RSA
Check WebCourses for the due date
Please work in pairs and put both people's names on each file submitted!

1) What is the prime factorization of 589449600?

2) What is $\varphi(589449600)$?

3) Using Fermat's Theorem, determine 3456^{25190} mod 2099.

4) Using Euler's Theorem, determine 13^{6051} mod 2664.

5) In an RSA scheme, p = 13, q = 31 and e = 127. What is d?

6) One of the primitive roots (also called generators) mod 29 is 2. There are 11 other primitive roots mod 29. One way to list these is 2^{a1} mod 29, 2^{a2} mod 29, … 2^{a12} mod 29, where $0 < a1 < a2 < \ldots < a12$. (Note: it's fairly easy to see that a1 = 1, since 2 is a primitive root.) Find the values of a10, a11 and a12 and the corresponding values 2^{a10} mod 29, 2^{a11} mod 29, and 2^{a12} mod 29.

7) (12 pts) In the Diffie-Hellman Key Exchange, let the public keys be p = 29, g = 19, and the secret keys be a = 11 and b = 13, where a is Alice's secret key and b is Bob's secret key. What value does Alice send Bob? What value does Bob send Alice? What is the secret key they share?

8) (10 pts) In El Gamal, Alice chooses $Y_A = \alpha^{XA}$ mod q. Bob, who is sending a message, calculates a value $K = Y_A^k$, where k is randomly chosen with $0 < k < q$. Is it possible that for different choices of k, Bob will calculate the same value K, or will each unique value of k be guaranteed to produce a different value for K? Give a brief rationale for your answer.

9) Write a program that prompts the user to enter an integer, n, in between 1 and 10^{12} and calculates $\varphi(n)$. **(Please write your program in either python or Java, which supports large integers. Please submit phi.py or phi.java.)**

10) 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.

(Please write your program in either python or Java, which supports large integers. Please submit primroot.py or primroot.java)

11) 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 $\varphi(p-1)$ 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.)

12) 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?

13) Decrypt the following message:

20429835450828679741350
26022799626812591980567
30572114224921561344399
14180424833673414562055
19539282983393676142312

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.