Fall 2018 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) What is the prime factorization of 6019208928?

2) What is φ(6019208928)?

3) Using Fermat's Theorem, determine the remainder when 15^{2992} is divided by 131.

4) Using Euler's Theorem, determine 701^{2689} mod 1224.

5) In an RSA scheme, p = 17, q = 29 and e = 143. What is d?

6) 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.)

7) One of the primitive roots (also called generators) mod 41 is 6. There are 15 other primitive roots mod 41. One way to list these is 6^{a1} mod 41, 6^{a2} mod 41, … 6^{a16} mod 41, where 0 < a1 < a2 < … < a16. (Note: it's fairly easy to see that a1 = 1, since 6 is a primitive root.) Find the values of a14, a15 and a16 and the corresponding remainders when 6^{a14}, 6^{a15} and 6^{a16} are divided by 41.

8) (12 pts) In the Diffie-Hellman Key Exchange, let the public keys be p = 37, g = 13, and the secret keys be a = 8 and b = 19, 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?

9) Write a program that attempts to factor the numbers below in the traditional way (trial division) and also using Fermat Factoring. Each of the numbers is the product of two primes. Time how long both methods take and produce a chart. Is there a clear advantage to the Fermat Factoring method over the traditional brute force method, according to your results? (Perhaps for a more accurate metric, count how many times the loops in both programs run and compare those numbers, include these values in your table as well, including the timing values.)

a) 441075437627829133

b) 733561193479131791

c) 611217877192686991

d) 1442059257386438303

e) 3008502085141882717