Fall 2019 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 1337834957760?

2) What is φ(1337834957760)?

3) Using Fermat's Theorem, determine the remainder when 135^{2672} is divided by 179.

4) Using Euler's Theorem, determine 7429^{628993} mod 529984.

5) In an RSA scheme, p = 31, q = 19 and e = 77. 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 43 is 29. There are 11 other primitive roots mod 43. One way to list these is 29^{a1} mod 41, 29^{a2} mod 41, … 29^{a12} mod 41, where 0 < a1 < a2 < … < a12. (Note: it's fairly easy to see that a1 = 1, since 29 is a primitive root.) Find the values of a10, a11 and a12 and the corresponding remainders when 29^{a10}, 29^{a11} and 29^{a12} are divided by 43.

8) In the Diffie-Hellman Key Exchange, let the public keys be p = 43, g = 20, and the secret keys be a = 25 and b = 29, 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) For this question, you are going to implement a RSA protocol to send the TAs and me (Arup) a message. For our RSA system, the public keys are as follows:

n = 135966249934813212187094231381
e = 43762348564782365746567456 7

Your message must be in Radix-64. Please google this format. It allows for 64 characters, encoding each with 6 bits. The characters are: all lowercase letters, all uppercase letters, all digits, the plus sign(+) and a forward slash (/).

First, type your message in a textfile only using those 64 characters. Type 16 characters per line. To encrypt, you will encrypt each line, one by one. Please pad the last line with '+' characters as needed. Convert each line of 16 Raxix-64 characters to a 96 bit integer. This will be your plaintext for RSA. Use the public keys given above and calculate the ciphertext, which will be a number from 1 to n-1. Output this number to a textfile. Do this for each line of the message. Here is what you need to turn in for this question:

1. Your code.

2. A text file with your ciphertext. This should have one number per line, for each block of 16 Radix-64 characters.

If you did everything to specification, the TAs and I should be able to read your message. **Please keep it clean =)** You may address any one of the three of us in your message, or all three of us, if you'd like!