Homework 2

This problem set is due January 30th.

Set-up for 1-3 The first few problems deal with the RSA encryption algorithm described here:

1. Alice picks two large primes (how one does this is nontrivial) and lets $n = pq$.
2. Alice then computes $\phi(n) = (p-1)(q-1)$
3. Alice then chooses a random integers e (how one does this is also nontrivial) so that $1 < e < \phi(n)$ and $gcd(e, \phi(n)) = 1$.
4. Alice find a solution $x = d$ to the equation
$$ex \equiv 1 \pmod{\phi(n)}.$$
5. Alice defines a function $E(x) : \mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ by
$$E(x) = x^e \in \mathbf{Z}/n\mathbf{Z}.$$

For this to be a secure encryption method, we have to assume that compute E^{-1} is hard. As far as we know, it is. I'll also point out that the pair ne is made public so that anyone can send messages to Alice.

Problem 1 Let n be an integer that is the product of distinct primes (i.e., is square-free). Also, let $d, e \in \mathbf{Z}_{>0}$ be such that $p - 1 | de - 1$ for each prime $p|n$. Show that $a^{de} \equiv a \pmod{n}$ for all $a \in \mathbf{Z}$. This d is the decryption key that Alice uses to decrypt messages sent to her.

Problem 2 As problem 1 shows, the decryption key can be found if the factorization of n is known. In this problem, show that if $\phi(n)$ is known, one can factor n. Do this by explaining why we know the coefficients of the polynomial
$$x^2 - (p+q)x + pq = (x-p)(x-q)$$
even though we know neither p nor q directly. From here, one could use the quadratic formula to find the roots

Problem 3 In order to use the RSA cryptosystem to encrypt messages, it is necessary to encode them as a sequence of numbers of size less than $n = pq$. We now describe a simple way to do this. Note that in any actual deployed implementation, it is crucial that you add extra random characters ("salt") at the beginning of each block of the message, so that the same plain text encodes differently each time. This helps thwart chosen plain text attacks. Suppose s is a sequence of capital letters and spaces, and that s does not begin with a space. We encode s as a number in base 27 as follows: a single space corresponds to 0, the letter A to 1, B to 2,... , Z to 26. Thus "RUN ALICE" would be the integer
$$27^8 \cdot 18 + 27^7 \cdot 21 + 27^6 \cdot 14 + 27^5 \cdot 0 + 27^4 \cdot 1 + 27^3 \cdot 12 + 27^2 \cdot 9 + 27^1 \cdot 3 + 27^0 \cdot 5.$$

Given $p = 17$ and $q = 19$, encrypt the letter X. Also, show the encryption followed by decryption gives X as well.

Problem 4 To compute $a^b \bmod n$, at most how many multiplications would it take using the repeated squaring technique from class?

Problem 5 Find the order of 7 mod 10. Show the 2 is a primitive root mod 11. Show that 20 has no primitive roots (try not to to do this one merely by brute force – Problem 6 may be relevant).

Problem 6 Show the following: If a and n are relatively prime integers with $n > 0$, then the positive integer x is a solution of the congruence $a^x \equiv 1 \pmod{n}$ iff the order of a mod n divides x.

Problem 7 Show the following: If a and n are relatively prime integers with $n > 0$, then $a^i \equiv a^j \pmod{n}$ (i and j are nonnegative integers) iff $i \equiv j \pmod{\text{order of a mod n}}$.

Problem 8 Was this set more reasonable than the first? Any other comments?