HOMEWORK ASSIGNMENT #6, DUE FRIDAY, 11/05/2010

This assignment has certain problems which require a fair amount of numerical calculation. For all problems but the first you can use a calculator, but you should explain your work. (In particular, it is fine if you use a calculator or computer to compute exponentials mod n, and you do not need to work out all the details of the fast exponentiation algorithm we did last week.)

(1) Compute the remainder when 5^{1636} is divided by 96. You should not need a calculator to solve this problem.

(2) Find all solutions to $\phi(n) = n/2$.

(3) The following message is encoded using a Caesar cipher which is just a linear shift of the alphabet. Decode the message; you should give some (but not too detailed) indication of how you decoded it: "SWOPDEOPDABWYAPDWPHWQJYDAZWPDKQOWJZODELO". Hint: this message is too brief to guarantee that 'e' is the most common letter in the unencrypted message, but another statistically frequent letter is (tied as) the most frequent letter in this message. The five most common letters, in descending order of frequency, are 'e', 't', 'a', 'o', 'i'. Extra credit (1 point): Who is the quote referring to?

(4) Suppose Julius Caesar decides to encode his messages by using a linear transformation $x \mod 26 \mapsto ax + b \mod 26$ instead of just the linear shift $x \mod 26 \mapsto x + b \mod 26$, where a, b are integers. What conditions (if any) must a, b satisfy to ensure that distinct encrypted messages are decrypted to distinct unencrypted messages? For these a, b, what is the decrypting transformation? Your answer will be in terms of a, b. (For instance, in the case where $x \mod 26 \mapsto x+b \mod 26$ is the encrypting transformation, the decrypting transformation is $x \mod 26 \mapsto x - b \mod 26$.)

(5) Suppose you are using RSA to receive encrypted messages. You select $p = 1987, q = 2297$ to generate your public key, and you use $e = 5$ as the encryption exponent, so that you publish $(1987 \cdot 2297, 5)$ as your public key. Someone sends you the message 4474044. Decode it.

(6) Suppose someone publishes $(10579, 3) = (N, e)$ as their public key, and you intercept a message '656' directed to that person. Decode the message. (To get an idea of the difficulties in breaking RSA, you should first try doing this problem without having a computer factor 10579 for you – rather, you should try to find a factor of 10579 using just a calculator and trial division.)

(7) Let $N = pq$ be the product of two distinct odd primes, and let $a \equiv 1 \mod \phi(N)$, where a is a positive integer. Show that $x^a \equiv x \mod N$, regardless of whether $\gcd(x, N) = 1$ or not. (This shows that when encoding and decoding a message x using the RSA cryptosystem, we don't need to worry about whether x is relatively prime to any particular number or not. Contrast this to the fact that we do need to worry about whether e is relatively prime to $\phi(N)$.)

(8) In contrast to the above problem, show that if N is an arbitrary integer, and $a \equiv 1 \mod \phi(N)$, it might not be the case that $x^a \equiv x \mod N$, for some choice of x. (Probably the easiest way to do this problem is to actually write down N, a, x, such that $a \equiv 1 \mod \phi(N)$ but $x^a \not\equiv x \mod N$.