HW 8 CMSC 389. DUE Jan 17

1. (0 points) READ my NOTES on RSA.

2. (30 points) Compute the following using the method in class Friday and in the RSA notes. Show all work. You can use a calculator.

   (a) $2^{100,000,000,000,000} \pmod{17}$

   (b) $3^{500,000,000,000,000} \pmod{47}$

   (c) $4^{200,000,000,000,000} \pmod{91}$

3. (30 points) In the problems below p, q, r are primes and a, b, c are ≥ 1.

   (a) Find a formula for $\phi(p^2q^2)$. Prove your result.

   (b) Find a formula for $\phi(p^aq^b)$. Prove your result.

   (c) Find a formula for $\phi(p^aq^br^c)$. Prove your result.

4. (30 points) Alice and Bob are going to use RSA with $p = 5$, $q = 7$ (so $pq = 35$ and $(p-1)(q-1) = 24$), and $e = 7$.

   (a) List all of the numbers in $\{1, \ldots, 23\}$ that are relatively prime to 24.

   (b) What value of d does Alice use? (its one of the numbers in the set in part 1, so you can do this by trial and error- ther are not that many of them.)

   (c) Bob wants to send the message 14. What does he send?

5. (10 points) Alice and Bob want to use RSA. Alice picks a random p, q but then picks an e that is NOT rel prime to $(p-1)(q-1)$. Why is this a TERRIBLE idea?