Math 565, Problem Set 4: *due Wednesday, January 31*

1. This problem is about the Euler totient function, ϕ.

   a) If p and q are distinct primes, how is $\phi(pq)$ related to $\phi(p)$ and $\phi(q)$?

   b) If p is prime, what is the value of $\phi(p^2)$? In general, determine a formula for $\phi(p^j)$ and prove that it is correct. (Hint: Among the numbers between 0 and $p^j - 1$, remove those with a factor of p. The ones that are left are relatively prime to p.)

   c) Let M and N be integers satisfying $\gcd(M, N) = 1$. Prove the multiplication formula:

   $$\phi(MN) = \phi(M)\phi(N).$$

   d) Let $p_1, p_2, \ldots, p_r$ be the distinct primes that divide N. Use your results from (b) and (c) to prove the following formula:

   $$\phi(N) = N \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

2. Let N, c, and e be positive integers satisfying the conditions $\gcd(N, c) = 1$ and $\gcd(e, \phi(N)) = 1$.

   a) Explain how to solve the congruence

   $$x^e \equiv c \pmod{N},$$

   assuming that you know the value of $\phi(N)$.

   b) Solve the following congruences, using the method you described in part (a):

      i) $x^{577} \equiv 60 \pmod{1463}$

      ii) $x^{959} \equiv 1583 \pmod{1625}$

      iii) $x^{133957} \equiv 224689 \pmod{2134440}$.

3. Here is a proposal for a cryptosystem: Alice chooses two large primes p and q and publishes $N = pq$, which is hard to factor. She also chooses three random integers g, r_1, r_2 and computes

   $$g_1 \equiv g^{r_1(p-1)} \pmod{N} \quad \text{and} \quad g_2 \equiv g^{r_2(q-1)} \pmod{N}.$$

Her public key is the triple (N, g_1, g_2), and her private key is the pair (p, q). When Bob wants to send a message $m \in \mathbb{Z}/N\mathbb{Z}$ to Alice, he chooses two random integers s_1 and s_2 and computes

$$c_1 \equiv m g_1^{s_1} \pmod{N} \quad \text{and} \quad c_2 \equiv m g_2^{s_2} \pmod{N}.$$

He then sends the ciphertext (c_1, c_2) to Alice. To decrypt, Alice simply solves the pair of congruences

$$x \equiv c_1 \pmod{p} \quad \text{and} \quad x \equiv c_2 \pmod{q}.$$

a) Prove that Alice's solution x is congruent to Bob's plaintext m modulo N.

b) Explain how Eve can easily break this cryptosystem.

4. Formulate a woman-in-the-middle attack, similar to that described in the text for the Diffie-Hellman key exchange, for the following cryptosystems:

   a) ElGamal

   b) RSA

5. Alice uses RSA with public key $N = 1889570071$. In order to guard against transmission errors, she has Bob encrypt his message twice, once using the encryption exponent $e_1 = 1021763679$ and once using the exponent $e_2 = 519424709$. Eve intercepts the two resulting ciphertexts

$$c_1 = 1244183534 \quad \text{and} \quad c_2 = 732959706.$$

   Assuming that Eve also knows N and the two encryption exponents e_1 and e_2, use the method described at the end of section 3.3 of the text to help Eve recover Bob's plaintext without finding a factorization of N.