MAT 301 Problem Set 3

[Posted: Feb 11, 2013. Due: Feb 25, 2013. Worth: 100 points]

1. **(10 points)** Solve the following problems.

   (a) Compute $2^{243} \pmod{455}$ using the Chinese remainder theorem. Show your work. `[You can use the fact that` $455 = 5 \cdot 7 \cdot 13$`.]`

   (b) I have a number of apples, I know that I don't have more than 1000 of them, but I don't have fewer than 900 either. When I arrange them in groups of 11, I have three left over. When I arrange them in groups of 13, I have five left over. How many apples do I have?

2. **(15 points)** Let $N = pq$ be a product of two distinct primes p and q. Suppose I give you N and the inverse of 3 mod $\phi(N)$. That is, I give you N and $d = 3^{-1} \pmod{\phi(N)}$, but I don't tell you what $\phi(N)$ is. Using this information, show a fast way to find the prime factors of N.

3. **(15 points)** Consider the following variant of a one-time pad. Fix a prime p. The secret key (that Alice and Bob have in common) is a pair of random numbers $(a, b) \in \mathbb{Z}_p$. To encrypt a message $m \in \mathbb{Z}_p$, they compute the ciphertext $c = am + b \pmod{p}$.

   (a) How many messages can they safely encrypt using this scheme? Prove your assertion.

   (b) Find the minimal number k such that given k messages together with their ciphertexts, you can quickly recover the secret key.

4. **(30 points)** The following two problems relate to the RSA encryption scheme.

   (a) Let N_1, N_2 and N_3 be distinct RSA moduli, such that $\mathsf{gcd}(3, \phi(N_1)) = \mathsf{gcd}(3, \phi(N_2)) = \mathsf{gcd}(3, \phi(N_3)) = 1$. and let $e = 3$. Show that given three vanilla RSA ciphertexts of a number $m < \mathsf{min}(N_1, N_2, N_3)$ under public keys (N_1, e), (N_2, e) and (N_3, e) respectively, one can quickly find the underlying message M. `[Clearly, you should accomplish this without factoring any of` N_1`,` N_2 `or` N_3`.]`

   (b) A *multiplicatively homomorphic* encryption scheme is one where given ciphertexts of two messages M_1 and M_2 (under the same public key), one can easily find a ciphertext that encrypts their product, namely $M_1 \cdot M_2$. Show that the vanilla RSA scheme is multiplicatively homomorphic.

5. **(30 points)** Answer the following two questions related to finding prime numbers and primality testing.

   (a) How does one generate safe prime pairs, that is, primes p and q such that $p = 2q + 1$? One way is to choose a random number q and test that it is prime (e.g., using Miller-Rabin). If it is prime, proceed to test that $p := 2q + 1$ is prime as well (again, using

Miller-Rabin). This works, but it invokes the primality testing algorithm twice. We'd like to show that safe prime pairs can be generated at the cost of a single primality test. Prove that if q is a prime, $p := 2q + 1$ is a prime if and only if $2^{p-1} = 1 \pmod{p}$. Use this to devise a faster way of generating safe prime pairs using a single primality test.

(b) Show that no number N of the form p^2q for distinct primes p and q can be a Carmichael number. `[You can use the fact that the group` $\mathbb{Z}_{p^2}^*$ `is cyclic, and therefore has a generator.]`

Challenge Question: This is an extension of question 5(b). Can you show that the padded RSA scheme is multiplicatively homomorphic?