Math 173A - Homework 2

1. Do the following exercises from the textbook. 2.5, 2.6, 2.7, 2.9.

2. Consider this combination of the Caesar cipher and the multiplication cipher briefly discussed in lecture, known as the *affine shift cipher*. Fix a prime p. The key for an affine cipher consists of two integers $k = (k_1, k_2)$ and encryption is defined by

$$e_k(m) = k_1 \cdot m + k_2 \pmod{p}.$$

   (a) What should the decryption function be?

   (b) For a fixed prime p, how many valid keys are there?

   (c) What are the message and ciphertext spaces?

   (d) Assuming that p is public knowledge, explain why the affine cipher is vulnerable to a known-plaintext attack? How many plaintext-ciphertext pairs are likely needed to recover they key?

3. Let's generalize the affine cipher from the previous exercise. Now suppose the plaintext m, ciphertext c, and the second part of the key k_2 are vectors consisting of n numbers modulo p. The first part of they key k_1 is an $n \times n$ matrix whose entries are integers modulo p. Encryption is defined by

$$e_k(m) = k_1 \cdot m + k_2 \pmod{p},$$

   where $k_1 \cdot m$ is the matrix-vector product.

   (a) What should the decryption function be?

   (b) How many valid keys are there? *Hint: are some matrices bad for this? How can you count the good ones?*

   (c) Why is this cipher vulnerable to a known-plaintext attack?

   (d) Explain how any simple substitution cipher that involves a permutation of the alphabet can be thought of as a special case of this cipher.

4. (a) Compute $6^5 \pmod{11}$ using the square-and-multiply algorithm.

   (b) Assume that 2 is a primitive root modulo 11 and suppose that $2^x \equiv 6 \pmod{11}$. *Without finding the value of x,* determine whether x is even or odd.

5. Recall that in the Elgamal protocol, every time Bob sends a message to Alice he generates a random exponent k. Suppose Bob is lazy and decides to use the same value of k for multiple messages. Explain why this renders his communications with Alice vulnerable to a known-plaintext attack.