SPCS CRYPTOGRAPHY
HOMEWORK 5

Please try all the unmarked problems. $\#, \star$ problems are both optional, with $\star$ problems being harder. You are strongly encouraged to work in groups, but you have to write up the solution on your own.

Reference for today's lecture: Chapter 4.4, Chapter 10.1-10.3 of textbook.

1. Alice has a bag of 500 candies. She just realizes that the bag was opened and a few candies were eaten. Coming from Mars, she has 13 fingers and 17 toes - a quick count shows that there are 2 candies left if she counts in groups of 13, and 3 candies left if she counts in groups of 17. Find the number of candies being eaten.

2. Find all the solutions of
   (a) $x^2 \equiv 1 \bmod 3$.
   (b) $x^2 \equiv 1 \bmod 7$.
   (c) $x^2 \equiv 1 \bmod 21$.
   (d) $x^2 \equiv 2 \bmod 21$.

3. Find the last two digits of 7^{2015}. (Hint: $100 = 4 \cdot 25$)

4. Alice and Bob decide to use the Diffie-Hellman key exchange with $p = 41$ and $g = 7$. Alice chooses $a = 14$, and Bob chooses $b = 23$. What is their shared key?

5. Bob wishes to send Alice a message encrypted with ElGamal encryption. They decide to use $p = 73$ and $g = 5$. Alice picks some a and computes the public key $g^a \equiv 49 \bmod p$. Bob chooses a random key $k = 33$ and wishes to send the message $m = 62$. What is the ciphertext he sends?

6. The *message expansion ratio* of a cryptosystem is
   $$\text{length of ciphertext} : \text{length of plaintext}.$$
   in the worst case. For example, the Caesar cipher has a message expansion ratio of 1-to-1, because the ciphertext has the same length as the plaintext. What is the message expansion ratio of
   (a) substitution cipher
   (b) Vigenere cipher
   (c) ElGamal cryptosystem?

7. Think about what discrete logarithm problem in $(\mathbb{Z}/m\mathbb{Z}, +)$ means, and whether it is a hard problem to solve.

8. Try to modify Diffie-Hellman so that it works for three people. In other words, Alice, Bob and Carol need to come up a way to have a shared secret key by communicating in a public channel.

9. You are Barack Obama. You are fighting with another country, and you want your three commanders to launch a missile only when all of them see fit.

   The missile launching system takes a secret code and will launch the missile if the correct code is entered. If the wrong code is entered, the whole system will blow up and US is in grave trouble.

   You have the secret code, a number close to 1000. Devise a way to give some information about the code to each of the three commanders, so that any two of them won't be able to figure the actual code out, but with all three of them they can. A (unrealistic) hint: use Chinese remainder theorem!