MATH 470 Homework 5 (Due October 4 **on Gradescope**)

Instructions:

- IF YOU LEAVE AN ANSWER BLANK, YOU WILL AUTOMATICALLY RECEIVE 2/5 POINTS. ANY ATTEMPTED SOLUTION WILL BE GRADED AS USUAL (AND POSSIBLY GET LESS THAN 2/5 POINTS). DOES NOT APPLY TO BONUS QUESTIONS.
- The writing of your homework submission should be done entirely on your own and you should be able to justify all of your writing in your own words.
- Show your work and write legibly. If there is any difficulty in reading or understanding your submission, or if any nontrivial steps are missing in your work, then points may be deducted.
- When you upload your submission to Gradescope, **make sure you match the correct page(s) for each question**. Otherwise your submission may not be graded, or points may be deducted.
- You may use an online calculator or code for the following operations:
  - add, subtract, multiply, quotient, remainder, rounding, non-modular square roots
  - (Extended) Euclidean Algorithm, fast powering

Required problems (in the SECOND edition of textbook: "An Introduction to Mathematical Cryptography", Second Edition, by Hoffstein, Pipher, and Silverman.)

1. (5 points) 3.7
2. (5 points) 3.9(a)
3. (5 points) 3.13
4. (5 points) 3.15(d,e)
5. (5 points) Show that the Elgamal encryption protocol is insecure against a Chosen Ciphertext Attack. More specifically, suppose Bob has published a prime p, primitive root g mod p, and his public key B. Alice has sent Bob a ciphertext (c_1, c_2). So far Eve only knows p, g, B, and (c_1, c_2). But suppose now that Eve can somehow make Bob decrypt "random-looking" ciphertexts (c_1', c_2') of Eve's choice (by "random-looking" we mean that Bob should not be able to tell that (c_1', c_2') or its decryption is related to Alice's message in any way). Show how Eve can use this ability to decrypt Alice's message.
6. (5 points) Let $N = pq$ be a product of two distinct odd primes p and q. Show that there are four square roots of 1 modulo N. In other words, show that there are exactly four integers in $\{1, 2, 3, \ldots, N-1\}$ whose squares are congruent to 1 mod N.
   (hint: use Chinese Remainder Theorem and Exercise 1.36(a). See also Example 2.28 in text.)
7. (Bonus 5 points) Suppose that you are given an integer N and a pair of integers e, d with the promise that N is the product of two large primes and that $ed \equiv 1 \mod \phi(N)$ (but you are not given the factors of N nor the value of $\phi(N)$). Describe an algorithm that efficiently factors N. (hint: use ideas from the Miller-Rabin test. Your algorithm should succeed with "high probability" in a similar sense as the Miller-Rabin test). You should explain at a high level why your algorithm works, but you don't have to give a complete proof.

Suggested practice problems (do not submit): 1.37, 2.21, 3.10