MATH 470 Homework 4 (Due September 13 **on Gradescope**)

Instructions:

- 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.
- For questions marked $*$ (e.g. 6^*.), you may write your own code (in any standard language) to solve the problem. But in this case you must write the code **from scratch** and attach a copy or screenshot of the working code together with the output in your submission.
  The only "built-in" mathematical functions you can use in the code are:
  - basic arithmetic operations: add, subtract, multiply, quotient, remainder
  - (Extended) Euclidean Algorithm, fast powering

  Any other mathematical function you want to use must be built by you using the above.
  If it is noticed that the output of your submitted code does not match your answer, this will be considered a violation of the Aggie Honor Code.

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

You can use a calculator/built-in function to compute large powers.

1. (5 points) 2.6 (you don't have to figure out Alice's secret exponent)
2. (5 points) 2.8(b,c)
3. (5 points) 2.9
4. (5 points) 2.17(a) (do this by hand)
5. (5 points) Let $p \geq 3$ be a prime and suppose that the congruence $X^2 \equiv b \pmod{p}$ has a solution. Prove that the congruence $X^2 \equiv b \pmod{p^2}$ also has a solution.
6. (5 points) Let p be a large prime and let g be a primitive root mod p. Suppose p and g are publicly known to everybody in a network. Alice chooses a secret integer a and publishes $A = g^a \mod p$ as her public key by broadcasting it over the network. Bob wants to send Alice a message m using Elgamal encryption.
   Suppose however that an active adversary Eve has the ability to intercept and modify messages sent over the network (including Alice's broadcasting of her public key) without being detected. Show how Eve can perform a Man-In-The-Middle attack.

7^*. (Bonus 5 points) You may assume that $p = 123456789001907$ is prime and that 2 is a primitive root modulo p. Find an integer x such that $2^x \equiv 3 \mod p$.

Suggested practice problems (do not submit): 1.36(d), 2.3, 2.7(a), 2.12, 2.16(b)