Homework 02

ECE 443/518, Fall 2024

Due Date: 10/06 (Sun.) by the end of the day (Chicago time)

1. *(1 point)* Solve Problem 12.3 (p329 in Understanding Cryptography).
2. *(1 point)* Alice chooses $p = 11$ and $q = 19$ to setup her RSA keys.
   A. Show that $e = 5$ is NOT a valid choice.
   B. Show that $e = 7$ is a valid choice. What is the public key and what is the corresponding private key?
   C. Suppose Bob want to send the message $x = 10$ to Alice using the keys generated in the question B. Show how Bob computes the ciphertext y and how Alice decrypts y.
3. *(1 point)* Bob setups his RSA key using $p = 13$, $q = 17$, and $e = 5$.
   A. What is the public key and what is the corresponding private key?
   B. For the question 2.C, if Bob want to sign his message $x = 10$, show how Bob computes the signature and how Alice verifies it.
4. *(1 point)* Solve Problem 8.5 (p235 in Understanding Cryptography).
5. *(1 point)* Solve Problem 13.11 (p355 in Understanding Cryptography).

Bonus. *(1 point)* Solve Problem 7.13 (p202 in Understanding Cryptography).