

Homework 03

ECE 443/518, Fall 2022

Due Date: 11:00am 10/05 Chicago time

1. (3 points) Solve Problem 11.2 (p315 in Understanding Cryptography).
 2. (2 points) Solve Problem 12.3 (p329 in Understanding Cryptography).
 3. (3 points) 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 .
 4. (2 points) 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 3.C, if Bob want to sign his message $x = 10$, show how Bob computes the signature and how Alice verifies it.
 5. (3 points) Solve Problem 8.5 (p235 in Understanding Cryptography).
 6. (2 points) Solve Problem 13.11 (p355 in Understanding Cryptography).
- Bonus. (3 points) Solve Problem 7.13 (p202 in Understanding Cryptography).