CSE 548 Spring 2024 Midterm

Your name: _____

You have an hour and 15 minutes (a regular class period) to complete this exam. Mark on this sheet of paper with a pen or pencil, and then turn it in at the front of the room to the TA or I. This test is closed book (note that there is no textbook for the course) and closed note except that you can have one 8.5” by 11” sheet of notes (written on front and back if you like). You may not use any electronic device (not even a calculator) and you may not communicate in any way with any individuals other than the instructor of the course and the TA during the exam. Any violation of these policies will result in a 0 on the exam and will be treated as an act of academic dishonesty as per the syllabus. Every question is worth 10 points. For multiple choice questions, circle the best answer. For short answer questions, write at least one word and at most one sentence in the blank space provided, and give the correct answer.

Example question #1

- For a simple XOR-based “encryption” scheme, like bitwise XOR the plaintext with the key to get the ciphertext, how would the receiver decrypt the plaintext?
  - A. XOR the ciphertext with the key
  - B. XOR the ciphertext with itself
  - C. Add the key to the letter, wrapping around from A to Z
  - D. With Galois fields

Example question #2

- Which of these encryption algorithms is purely symmetric?
  - A. Diffie-Hellman
  - B. RSA
  - C. AES
  - D. None of the above