CS 429 Homework 2

Name: ___________________________ Section #: ___________________________

Instructions: Type the answers into a file and submit on Canvas. As usual, you may collaborate with your classmates and ask for assistance from the TA. But don’t copy anyone else’s answer. Each problem is worth the same number of points (more or less).

1. Convert between binary and decimal representations:
   (a) 11.475 to binary
   (b) Binary 110000011001111 to hexadecimal
   (c) Binary 101.1111 to decimal

2. Show the result of rounding to the nearest 1/8 according to the round-to-even rule:
   (a) 11.0001
   (b) 11.0010

3. We have a 9bit FP representation based on the IEEE 754 standard: 1 for the sign, 4 for the exponent and 4 for the fraction. You may need to round. You should show your work for partial credit. Please show answers in binary.
   (a) Represent 0.125 (1/8) in this system.
   (b) Represent 5.25 in this system.
   (c) Obtain the product of the two numbers from (a) and (b) above:
      - Add the two exponents using exponent encoding: __________________________
      - Multiply the two significands including rounding: __________________________
      - Give the result in 9-bit binary format. __________________________
   (d) Obtain the sum:
      - Normalize so both have same exponent: __________________________
      - Now show the sum, which may require normalizing exp or rounding.

4. Extra Credit: Prove by induction that sign extension preserves the value.

5. Extra Credit: An encryption method called one time pad is regarded as a perfect cipher. To send bit string P (the plaintext) securely across a channel do the following: Agree with the recipient in advance on a randomly generated bit string K of the same length as C. Send ciphertext C = (P ⊕ K), i.e., xor’d with K.
(a) How does the receiver extract P from the ciphertext?

(b) This is regarded as a perfect cipher—an attacker who doesn’t know the key has exactly the same chance of guessing the plaintext whether or not he has access to the ciphertext. That is, the ciphertext provides no information about the plaintext (except its length). Explain why that is. (Hint: think about sending a 3-bit plaintext string using this scheme.)

(c) Why is it important that the key be randomly generated?

(d) It’s called a one time pad for a reason. If you reuse the same key even once, the security is greatly reduced. Make an argument why that’s true.