CS 478/513: Computer Security
Spring 2022
Total Points: 100
Assignment 2

Due: Wed. 2/23, 11:59 pm

Please complete the following problems, being sure to justify/explain your steps and reasoning in all your answers. Your solutions must be submitted to Canvas as a PDF file.

This assignment is to be completed individually. Please cite your references used (except textbook), as described in the syllabus.

Chapter 3:

1. (5 points) Complete Problem 2 (a, b) from the text.
2. (10 points) Complete Problem 3 (a, b) from the text.
3. (15 points) Complete Problem 4 (all sub-parts) from the text.
4. (5 points) Complete Problem 11 (all sub-parts) from the text.
5. (5 points) Complete Problem 16 from the text.
6. (10 points) Complete Problem 18 (a, b) from the text.
7. (10 points) Complete Problem 22 (a, b) from the text.
8. (10 points) Complete Problem 24 from the text.
9. (10 points) Complete Problem 25 (a, b) from the text.
10. (10 points) Complete Problem 31 (a, b, c) from the text.
11. (10 points) Assume a particular Feistel cipher uses the round function $F(X, K) = X \oplus K$, and number of rounds $n = 4$. Let the plaintext block P be the 8-bit binary number 10110101, and the subkeys K_1 through K_4 as follows: 1011, 0100, 0101, 1010. Run the cipher on this input, and show the values of L_i and R_i for each round i, as well as the final ciphertext block that is obtained. *You do not have to compute each step by hand — you may write a simple program which gives the required outputs.* If you choose to write a program, please submit your source code, and README file, along with the rest of the assignment as a .zip file.