CS 478/513: Computer Security
Spring 2020
Total Points: 100
Homework 1

Due: Tue., 2/27/20, before class

Please complete the following problems, being sure to explain your conclusions or show your work when such details are requested. Your solutions must be submitted to Canvas as a PDF file.

This assignment is to be completed individually — plagiarism and cheating are strictly prohibited and are punishable. Please cite your references (except textbook), as described in the syllabus.

Chapter 1:

1. (5 points) Consider the definitions of confidentiality, integrity, and availability.
   (a) When might each of these aspects of information security be more important than the others?
   (b) Describe a few situations where strengthening one of these might weaken another.

Chapter 2:

2. (5 points) Complete Problem 19 (a, b) from the text.
3. (5 points) Complete Problem 29 (a, b, c, d) from the text.
4. (10 points) Suppose a cipher uses an 8-character mixed-case alphanumeric key (0-9, a-z, and A-Z).
   (a) What is the size of the keyspace (i.e., how many unique keys are possible)?
   (b) What is the approximate strength of the key, measured in bits? *Hint: rewrite the size of the keyspace as a power of two.*
   (c) If a particular computer can test 2^{40} keys per second, how long will it take (on average) to guess the key of this cipher?
5. (5 points) Consider that the 8-character key from the previous problem would take up 64 bits if stored as an ASCII string. However, in this scenario, not every bit would contribute to the strength of the key. Assume the cipher is upgraded to use all 64 bits.
   (a) What is the new size of the keyspace?
   (b) How much time would it take to crack the new version of the cipher (if able to test 2^{40} keys per second)?

Chapter 3:

6. (5 points) Complete Problem 2 (a, b) from the text.
7. (5 points) Complete Problem 3 (a, b) from the text.
8. (5 points) Complete Problem 11 (a, b, c, d) from the text.
9. (5 points) Complete Problem 16 from the text.
10. (10 points) Complete Problem 22 (a, b) from the text. Explain the reasoning behind your answer for part (a).
11. (10 points) Complete Problem 25 (a, b) from the text.
12. (10 points) Complete Problem 31 (a, b, c) from the text. Provide rationale to defend your answer for part (c).
13. (5 points) Complete Problem 36 (c) from the text. Explain why or why not.
14. (5 points) Complete Problem 41 (b) from the text. Show the work or formulas used to obtain the answer.

15. (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.*