CS 478/513: Computer Security
Spring 2022
Total Points: 100
Homework 1

Due: Tue., 2/9/22, 11:59 pm

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. (20 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.
   Answers may vary. One approach is to use the textbook's AOB as an example, and explain the 3 properties w.r.t. that.

Chapter 2:

2. (10 points) Complete Problem 19 (a, b) from the text.
   Sol: 19 a) Key is LKISTL, 19 b) Key is LEKEKR.
3. (20 points) Complete Problem 29 (a, b, c, d) from the text.
   Sol: 29 a) On an average, try $\frac{2^{40}}{2^1} = 2^{39}$ keys for a successful brute-force attack.
   29 b) For a given key, see how many valid words it produces (use a dictionary for reference). Key that produces max. number of valid words is the right key.
   29 c) Need to try 2^{39} keys. Beyond that, an efficient implementation of the dictionary as a hash table would require $O(1)$ lookup time.
   29 d) Depends on the length of the message. As we try more keys, the number of false negatives will be expected to decrease.
4. (30 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)?
   Sol: 10 + 26 + 26 = 62 unique characters. Size of keyspace is 62^8.
   (b) What is the approximate strength of the key, measured in bits? *Hint: rewrite the size of the keyspace as a power of two.*
   Sol: Key strength is 48 bits. So keyspace is 2^{48}.
   (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?
   Sol: It would take $\frac{2^{48}}{2^{40}} = 2^8$ seconds. On an average, it will take $\frac{2^8}{2} = 2^7 = 128$ seconds.
5. (20 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?
   Sol: New keyspace is 2^{64}.
   (b) How much time would it take to crack the new version of the cipher (if able to test 2^{40} keys per second)?
   Sol: It would take $\frac{2^{64}}{2^{40}} = 2^{24}$ seconds. On an average, it will take $\frac{2^{24}}{2} = 2^{23}$ seconds.