Computer Security
Homework 1

Due: 16^{th} March, 2018

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.

Chapter 1:

1. Complete Problem 10 (a, b) from the text. *The German Enigma is...*
2. 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:

3. Complete Problem 8 (a, b, c, d) from the text. *This problem deals with the concepts of confusion...*
4. Complete Problem 19 (a, b) from the text. *Using the letter encodings in Table 2.1, the following...*
5. Complete Problem 29 (a, b, c, d) from the text. *Suppose that Alice encrypted a message with a...*
6. Suppose a cipher uses a 10-character mixed-case alphanumeric key (0-9, a-z, 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?