**CS 4732/57322 Homework #1**

***Due electronically by midnight 6/21/2020***.

For submission, if done on paper please scan and submit as a pdf. If done in word, please submit the .docx or .doc format.

**IMPORTANT**: Clearly indicate outside resources utilized and sign below. Failure to cite use of outside resources will be reported for appropriate disciplinary actions. Note that discussions with other students are encouraged; copying – with or without modifications – is unacceptable and will also be reported.

I discussed one or more problems with the following people:

I hereby certify that any outside resources utilized, other than the textbook and class materials, are clearly cited. All other material I provide for this homework submission is my own original work.

*Printed name*

1. (8 points) In regards to the requirements of computer security:

a) What is the difference between confidentiality and integrity?

b) Give an example of some scheme that would protect integrity but not give confidentiality and vice versa.

2. (4 points) Suppose an organization could not break the encryption used by another organization. What other possible technique could they use to try and gain information?

3. (5 points) Describe security by obscurity. Does this conflict with any security design principles? If so, list the ones that it violates.

4. (9 points) Assign low, moderate, or high impact level for the loss of confidentiality, availability, and integrity of an organization that handles student loan data for students at a university. Justify your answers.

5. (10 points) Write an attack tree for getting into a professor’s office to steal his plushie dog that was abandoned during quarantine. Do not try this in practice.

6. (6 points) Describe the difference between a substitution and a transposition cipher. Give an example of a substitution cipher. Justify that it is not a transposition cipher.

7. (6 points) What problem does the autokey system of the vigenere cipher try to solve? Does it successfully solve the problem? If not, why not.

8. (6 points) Describe why a one-time pad is completely unbreakable. What happens if we try and brute-force something encrypted with a one-time pad?

9. (8 points) Encrypt the message “fullcredit” using the key “cat” using the vignere cipher.