**CS 4732/5732 Homework #1**

***Due electronically by midnight 6/23/2025***.

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*

Jamie Harris

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

a) What is the difference between confidentiality and integrity?

Confidentiality is the idea that information is not made available to people or systems that do not have authorization to access that information. Integrity is the idea that data or systems are not accessed or utilized in a way that was not intended or authorized.

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

A system that would favor integrity over confidentiality could be one that doesn’t allow users to modify or remove data, but has the data available for everyone to see.

A system that would favor confidentiality over integrity could be one that only allows certain users to see certain data, but also allows those users to do virtually whatever they want with or to the data.

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?

The organization could use a technique such as traffic analysis to get some ideas as to who, when, and where information is sent to and from.

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

Security by obscurity is a security method where the mechanisms of security are not made known to the outside. This violates the design principle of open design, because the security mechanisms are not knowable by outside observers, and could potentially also violate the principle of psychological acceptability due to the fact that if a user does not know the way in which the system is being secured, they may not find the security suitable.

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.

High – Availability: If the system’s availability is compromised, then students may not be able to access loan data and may lose some financial aid, or the university may not be able to properly request funds from state and federal governments for the loan amounts.

Medium – Integrity: If the system’s integrity is compromised, then loans could be deleted, or the balance on the loan could be drastically increased, which could harm both the students and the univerity financially

Low – Confidentiality: While it would be bad for the personal information of borrowers (names, social security numbers, etc) to be accessible by unauthorized users, it would not prevent the students or university from being able to properly utilize the loan funds.

5. (10 points) Write an attack tree for getting into a professor’s office to steal his plushie dog that was abandoned during summer break. 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.

A substitution cipher is a cipher that substitutes each letter in the message with another letter using a key as reference. A transposition cipher changes the order of the letters in the message, but it doesn’t change what letters are in the message. The Caesar cipher is a classic example of a substitution cipher, where each letter in the message is substituted with the letter 3 spaces ahead in the alphabet. This is not a transposition cipher, as it does not change the order of the characters, and two- or three-letter combinations still have the same relationship (i.e. AT would be DW, where A and D have the same distance from T and W respectively).

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.

The autokey system tries to solve the issue of letter frequency giving cryptanalysts the ability to more easily crack the cipher. However, it doesn’t adequately solve this problem. By having the key followed by the message itself in the enciphering code, there is a larger risk of a letter being used to encipher itself, especially with frequent letters such as ‘e’ and ‘t’.

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

One-time pad is unbreakable because the cipher and message are completely unrelated, and the random letter keys for each letter in the message mean that there is absolutely no information to go off of, such as letter frequency. If you try to brute force a one-time pad enciphered message, you will have no way of knowing if you’ve correctly deciphered the message, because as you go through the brute-force, you will get every possible message of that key’s length.

9. (8 points) Encrypt the message “cicada” using the key “dog” using the vigenere cipher. Show your work.

3 14 6 3 14 6

D O G D O G

C I C A D A

2 8 2 0 3 0

------------------------

5 22 8 3 17 6

F W I D R G