CS 4920/5920 Spring 2021
HW 1

HW 1 is due on 2/4. Explain how you reached your answers. Answers without explanations will receive no to little credit.

For the HW 1 submission, submit a zip file including your Answer sheet/doc/pdf and your code and files for the Cipher Programming problem.

Problem 1. CIA Triad

Consider a desktop publishing system used to produce documents for various organizations.

a. Give an example of a type of publication for which confidentiality of the stored data is the most important requirement and explain why.
b. Give an example of a type of publication for which data integrity is the most important requirement and explain why.
c. Give an example in which system availability is the most important requirement and explain why.

Problem 2. Security News

Read the news about a security incident. Identify which of the confidentiality, integrity, availability, authenticity, and accountability are relevant, indicate the degree of importance, and explain why.

Cite the news source and have your answer in a couple paragraphs where one paragraph summarizes and explains the security incident and another paragraph discusses the CIA triad and authenticity and accountability.

Problem 3. Affine Caesar Cipher

A generalization of the Caesar cipher, known as the affine Caesar cipher, has the following form: for each plaintext letter p (where p can be an integer between 0 and 25 inclusive), substitute the ciphertext letter C:

$$C = \mathrm{E}([a, b], p) = (ap + b) \bmod 26$$

A basic requirement of any encryption algorithm is that it needs to be one-to-one. That is, if $p \neq q$, then $\mathrm{E}(k,p) \neq \mathrm{E}(k,q)$. Otherwise, decryption is impossible, because more than one plaintext character maps into the same ciphertext character. The affine Caesar cipher is not one-to-one for all values of a. For example, for a=2 and b=3, then $\mathrm{E}([a,b],0) = \mathrm{E}([a,b],13) = 3$.

a. Are there any limitations on the value of b for the affine Caesar cipher to be one-to-one? Explain why or why not.
b. What are the limitations on the value of b for the affine Caesar cipher to provide distinct mappings? Hint: Because of the mod-26 operation, some b provide equal mappings for the affine Caesar cipher.
c. Determine which values of a are not allowed.
d. Provide a general statement of which values of a are and are not allowed. Justify your statement.
e. How many one-to-one and distinct affine Caesar ciphers are there?
f. A ciphertext has been generated with an affine Caesar cipher. The most frequent letter of the ciphertext is "A", and the second most frequent letter of the ciphertext is "X." Break this code.

Problem 4. Cipher Programming

For this programming problem, include your code with comments, the compiler output or the executables (if applicable), the input and the output files. You should write your program in C++, C, Java, Python, or Matlab.

Write a program that can encrypt and decrypt using the general Caesar cipher (not the Affine Caesar cipher), also known as an additive Caesar cipher.

a. Describe your program/implementation in your Answer sheet/doc/pdf. The description should include what your program does, the program input/output, and the file/data format description, etc.
b. Generate two input test files. Each file should have at least 50 letters. (2 files)
c. Generate the two output files to your input files from the previous part. (2 files)

Write a program that can encrypt and decrypt Hill cipher. For your hill cipher, append a “q” to the end of the message (if needed) and ignore the non-letter symbols (such as “.”). Specify and describe the other rules in your Program Description.

d. Describe your program/implementation in your Answer sheet/doc/pdf. The description should include what your program does, the program input/output, and the file/data format description, etc.
e. Encrypt the message “crypto is at four forty five but it is virtual this semester. hopefully we can get back to our normal mode” using the Hill cipher with the key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$. Include your output file. (1 file)
f. Generate one input test file and the corresponding output file. The input file should have at least 50 letters. (2 files)

The following are further guidelines (updated on 1/28/2021):

- Make your code generalizable, for example, Hill cipher can use a m x m matrix as the key
- Your input file should include all the parameter variables (e.g., the key), as opposed to having them on separate files or inputs, and the Program Description should specify the input file format (e.g., separate lines for the key and the plaintext). Your input file should provide sufficient information for us to generate the corresponding output using your program.
- For your file submissions, have them in .txt files and name your files according to the following naming scheme:

  “[Last_name]_[input/output]_Caesar_[File_number]” for the Caesar cipher
  “[Last_name]_[input/output]_Hill_[File_number]” for the Hill cipher

  For example, if your name is John Doe, then the files for Part b would be “Doe_input_Caesar_1.txt” and “Doe_input_Caesar_2.txt” while the files for Part c would be “Doe_output_Caesar_1.txt” and “Doe_output_Caesar_2.txt”

Problem 5. Playfair Cipher

a. Using this Playfair matrix:

R	T	O	P	Q
X	Z	U	V	W
Y	K	E	A	S
F	G	B	C	D
M	N	H	I/J	L

Encrypt this message (ignore capitalization and append a 'x' to the end of the message if needed):

Everyone stay healthy

b. Repeat part a. using the Playfair matrix with the key *easykey*.
c. How do you account for the results of this problem? Can you generalize your conclusion?
d. How many possible keys does the Playfair cipher have? Ignore the fact that some keys might produce identical encryption results. Express your answer as an approximate power of 2.
e. Now take into account the fact that some Playfair keys produce the same encryption results. How many effectively unique keys does the Playfair cipher have?

Problem 6.

a. Explain the difference between a monoalphabetic cipher and a polyalphabetic cipher.
b. Using Vigenere cipher, encrypt the word "questionsandanswers" using the key *matrix*.

The rest of the problem explores the use of a one-time pad version of the Vigenere cipher. In this scheme, the key is a stream of random numbers between 0 and 25. For example, if the key is 3 19 5 …, then the first letter of plaintext is encrypted with a shift of 3 letters, the second with a shift of 19 letters, the third with a shift of 5 letters, and so on.

c. Encrypt the plaintext sendmoremoney with the key stream

9 0 1 7 23 15 21 14 11 11 2 8 9

d. Using the ciphertext produced in the previous part, find a key so that the cipher text decrypts to the plaintext cashnotneeded.

e. Can a brute-force attacker (not knowing the key in advance) decrypt the ciphertext from the previous part in a deterministic manner?