CS 4920/5920 Spring 2022
HW 1

HW 1 is due on 2/2. 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 1. CIA Triad

For the following scenarios, give examples of confidentiality, integrity, and availability requirements associated with the system and, in each case, indicate the degree of importance of the requirements and explain why.

a. An automated teller machine (ATM) in which user provide a personal identification number (PIN) and a card for account access
b. A telephone switching system that routes calls through a switching network based on the telephone number requested by the caller
c. An implanted defibrillator that uses a remote programmer to perform diagnostics, read/write data, and adjust the treatment settings

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 including one paragraph to summarize and explain the security incident and another paragraph to discuss 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. 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 'q' to the end of the message if needed):

Attend crypto class and 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?

Problems 5 and 6. The following problems are programming problems.

For the programming problems, 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. The following are further submission guidelines:

- Make your code generalizable, for example, Hill cipher can use a *m* x *m* matrix as the key for some number *m*.
- The class input files are used for both problems, e.g., encrypt the same messages using different ciphers. For example, "class_input_b.txt" is used for Parts b in both Problems 5 and 6.
- **Input format:** The first line includes the letters for the key (there will be m^2 number of letters for some number *m*). The Caesar in Problem 5 cipher only uses the first letter. The Hill cipher in Problem 6 constructs the key matrix row by row; for example, "jefh" corresponds to the key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$. The second line includes the message in plaintext.
- **Output format:** The output file has only one line including the ciphertext without the key.
- **Naming scheme:** For your file submissions, have them in .txt files and name your files according to the following naming scheme:

  "[Last_name]_[input/output]_[Problem_Part]"

  For example, if your name is John Doe, then the files for Part b for Problem 5 Caesar Cipher would be "Doe_output_5b.txt" while the files for Part d for Problem 5 would be "Doe_input_5d.txt" and "Doe_output_5d.txt". Only Problem Part d's using your own testing inputs include both input and output files, while the rest of the parts only include the output files.

Problem 5. Cipher Programming: Caesar Cipher

Write a program that can encrypt and decrypt using the general Caesar cipher described in the Textbook Section 3.2 (not the Affine Caesar Cipher). Ignore the non-letter symbols (such as "." And "").

a. Describe your program/implementation including: the description of your approach, the descriptions and references to the online resources/libraries you used, the definitions of the functions and variables, and the pseudocode.

b. Encrypt the text in the class-common input file ("class_input_b.txt") provided for this assignment. Generate the ciphertext in txt file. (1 file)

c. Decrypt the text in the class-common input file ("class_input_c.txt") provided for this assignment. Generate the decrypted plaintext in txt file. (1 file)

d. Generate one input test file on your own and encrypt it to generate the corresponding output file. The input file should have at least 50 letters. Also, verify that the decryption results back in to the plaintext message. (2 files)

Problem 6. Cipher Programming: Hill Cipher

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

a. Describe your program/implementation including: the description of your approach, the descriptions and references to the online resources/libraries you used, the definitions of the functions and variables, and the pseudocode.

b. Encrypt the text in the class-common input file ("class_input_b.txt") provided for this assignment. Generate the ciphtertext in txt file. (1 file)

c. Decrypt the text in the class-common input file ("class_input_c.txt") provided for this assignment. Generate the decrypted plaintext in txt file. (1 file)

d. Generate one input test file on your own and encrypt it to generate the corresponding output file. The input file should have at least 50 letters. Also, verify that the decryption results back in to the plaintext message. (2 files)