CS 491 / 591 Spring 2021
Homework 1 DUE April 6 AOE
Submit your homework by email to: yasodhan@pdx.edu
Please use this subject line: IntroSec HW 1 Submission

Part A: Written Exercises (40 points)

1. (10 points) Read this online article from Ars Technica: https://arstechnica.com/gadgets/2021/03/attackers-are-trying-awfully-hard-to-backdoor-ios-developers-macs/
a. Say how the XCodeSpy attack relates to any of the CIA: confidentiality, integrity, availability.
b. Say how the XCodeSpy attack relates to any of the STRIDE categories of threats.

2. (10 points each) Provide 2 references to computer security that you find in the non-technical space. For each of the 2 references:
a. Provide or describe what is said.
b. (5 points) Say how it relates to any of the CIA: confidentiality, integrity, availability.
c. (5 points) Say how it relates to any of the STRIDE categories of threats.

- Examples might be fiction, tv shows, movies, magazines, blogs, even news.
- The reference may be technically correct or incorrect, or maybe you don't know which.
- Include the source – movie name and year; tv name, year, seasons#, episode #; URL, etc. If possible, give a link. A link to an entire movie is NOT useful although your graders would probably enjoy watching all of those movies.

Note: as always, please filter out obscenity and hatred for the learning community.

3. (10 points) Draw an attack tree that describes a cheating student obtaining the answers to another student's homework. Include all paths you can think of.

Part B: Hands On: Vigenère Ciphers (60 points)

As a "warmup" to C programming, we will have some fun and implement a simple form of encryption called Vigenère Ciphers. In addition to a C refresh, the goal is to explore the challenge of letter frequency in particular, and patterns in particular, for simple encryption algorithms.

1. This programming exercise must be done in C. It will be a review or quick intro to C programming in a Linux environment.

2. Turn in your source code and a makefile as attachments to your homework email.
3. We will test and run your code on the Linux lab machines. If you want to work on those machines you can ssh to linuxlab.cs.pdx.edu. This machine name will switch you to a particular linux lab machine each time you login. Your home directory is the same across all machines.
4. To learn what a Vigenere Cipher is, see Wikipedia Vigenère Cipher

```
Here is a table of the relative frequency of letters in English text:

A: 8.167%
B: 1.492%
C: 2.782%
D: 4.253%
E: 12.702%
F: 2.228%
G: 2.015%
H: 6.094%
I: 6.996%
J: 0.153%
K: 0.772%
L: 4.025%
M: 2.406%
N: 6.749%
O: 7.507%
P: 1.929%
Q: 0.095%
R: 5.987%
S: 6.327%
T: 9.056%
U: 2.758%
V: 0.978%
W: 2.360%
X: 0.150%
Y: 1.974%
Z: 0.074%
```

Here is some plaintext:

ethicslawanduniversitypoliciestodefendasystemyouneedtobeabletothinklikeanattackerandthatinc
ludesunderstandingtechniquesthatcanbeusedtocompromisesecurityhoweverusingthosetechniqu
esintherealworldmayviolatethelawandtheuniversitycomputingpracticesormaybeunethicalyoumu
strespecttheprivacyandpropertyrightsofothersatalltimesorelseyouwillfailthecourseundersomecirc
umstancesevenprobingforweaknessesmayresultinseverepenaltiesuptoandincludingcivilfinesexp
ulsionandjailtimecarefullyreadthecomputerfraudandabuseactcfaaafederalstatutethatbroadlycrimi
nalizescomputerintrusionsthisisjustoneofseverallawsthatgovernhackingunderstandwhatthelawpr
ohibitsyoudontwanttoendupliketheguyifindoubticanreferyoutoanattorneypleasereviewcaenspolic

ydocumentonrightsandresponsibilitiesforguidelinesconcerninguseoftechnologyresourcesatpsuas membersoftheuniversityyouarerequiredtoadheretothesepolicies

1. [12 points] What are the frequencies of the letters in the plaintext? Write a C program that reads in text from a file into a buffer, counts the occurrences of each [lowercase] letter of the English alphabet, and computes the relative frequencies. Your program should print out the contents of the buffer, and the frequency results in a simple list such as the one above.
2. [12 points] Add a function to encrypt the plaintext with a Vigenere cipher and a given key. You should add the key as a command line argument so that you can enter a different key each time you run. A key is a text string of max length 4, min length 1.
3. [12 points] Add the functionality to count the occurrences of each [lowercase] letter of the English alphabet in the ciphertext, compute the relative frequencies, and print out the ciphertext and the frequency results in a simple list.
4. [12 points] Run your encryption program over the plaintext for two different keys: yz and wxyz.
5. [12 points] Submit a table of your results, First column is the alphabet, second is the relative frequency of each, 3rd column is frequency from plaintext, 4th column is frequency from key yz, and 5th column is frequency from key wxyz.
6. [no points, just wisdom, nothing to turn in] what happens to your program if the text in your file is too long to fit in the buffer? If you try to enter a key with length 5?