CptS 427/527 Assignment #2 – Cryptography and Cipher Algorithms

Due: March 31, 2022 by 11:59 PM

Submission Instructions:

You are free to use any methods or tools to solve the following questions, but you must document your work such that it could be repeated by someone else. Things to include:

- The names of any programs, tools, websites, or other sources you use
- Source code of any programs you write, including command line interface tools
- Screenshots of program output
- Pictures or manual calculations

Summarize the answers to each problem at the top of the page, then expand on how you arrived at each answer in subsequent sections below your answer summary. For example:

1. The Empire Strikes Back
2. Beren and Luthien
3. 10 PRINT CHR$(205.5+RND(1)); : 20 GOTO 10

1.

This question asked, "Which is the best Star Wars movie?" Because this question is only an opinion, I picked my favorite Star Wars movie from a list of all the Star Wars movies at https://en.wikipedia.org/wiki/List_of_Star_Wars_films.

2.

The second question asks to name the two main characters in J.R.R. Tolkien's book, "The Silmarillion". Because the Silmarillion is actually a collection of poems from the First Age, there could be multiple "main characters"; Illuvatar and Manwe, Manwe and Morgoth, Morgoth and Gil-galad, or many other pairs could all be potential answers. Because the title of the book refers to the Silmarils, and Beren is tasked with stealing one, I chose Beren and Luthien.

3.

The last question asked us to generate a random maze using Microsoft Basic V2 on the Commodore 64. It turns out this is a well-known program that was included in both the User Guide and the Programmer's Guide. Additionally, the program has received academic treatment in the book by the same name[1] as the one-line program.

[1] https://mitpress.mit.edu/books/10-print-chr2055rnd1-goto-10

… and now, The Real Questions!

Each question will get progressively harder. Don't overthink question #1. The answer (output) of each question will be used as input in the following question.

Question #1—Decode this simple monoalphabetic substitution cipher, which is the title of a book:

ACVLQDMZ

Question #2—Decode the monoalphabetic substitution cipher in question2.txt. The resulting keyword is related to the keyword from question #1.

Hint: You will need to perform cryptanalysis on the text. Carriage returns have been preserved, and only alphabetical characters are encrypted. All other symbols (e.g., spaces and punctuation) have been replaced with a '?', so ignore them.

Writing a program and testing the plaintext output often will be helpful.

Question #3—Decode this polyalphabetic cipher using the keyword from question2.txt. (The cipher itself has a connection to the plaintext in question #2.)

YSFKFMEOE

Question #4—What is in the question4.txt file? Use the keyword from question #3 to unzip question4.zip.

Application-level passwords are often used in place of native encryption. This is a bad practice for several reasons. When comingled with unprotected documents, protected documents indicate their value. The specific application can also be targeted to break the protection.

As the price of computation continues to fall, a strong argument for confidentiality is to encrypt everything.