Adrian Ward-Manthey

Jeff Blankenship

March 27, 2017

CS 492 Security

How to use our project

Our project can be used to encrypt and decrypt a text file via a simple substitution cipher. Our project consists of two interconnected HTML pages (links at the bottom of each page allows you to go to back and forth between the pages). One page allows you to encrypt a text file while the other pages offers various options for decrypting a text file.

To begin, run the file index.html and click the link at the bottom to go to the encryption page.

**Encryption**:

To encrypt a text file, you will need to be on that HTML page entitled “Ceasar Tool: Text file encrypter”. On the top of the page, click the “Choose File” button and select your desired text file from your computer. Click “Load File” to load the file into the Plaintext field.

You can choose your key in **THREE** different ways. Clicking the “Randomize” button uses a random number generator to create a randomized key. If you want to use and arithmetic offset, you can either type an offset value between 0-25 in the offset field or hover your cursor over the offset field and use the arrows to choose a number. Lastly, you can type in a substitution key yourself in the field next to randomize.

Once you’ve decided on your key, simply click the “Encrypt” button to encrypt the Plaintext file. The “Frequency Order” field simply tells you the frequency of characters (from greatest to least) in the plaintext. To save the ciphertext, type in a file name in the “File to Save As” field and click the “Save Cypher” button to save the file onto your computer.

**Decryption**:

To decrypt a text file, you will need to be on that HTML page entitled “Caesar Tool: Simple Sub cryptanalyzer”. On the top of the page, click the “Choose File” button and select your desired text file from your computer. Click “Load File” to load the file into the cyphertext field.

You have several different options to decrypt. The first thing you should do is look underneath the plaintext text field and click on “Choose File” (it’s next to the text that says “Dictionary File”). You will need to load in a dictionary file (a text file of a dictionary) if you want to use the brute force button.

You have **THREE** options to choose from for decrypting a cyphertext. The ***first option*** is to click the “Use Frequencies” button. The “Frequency Order in use:” text field contains a default value for frequency of characters in the English language (from greatest to least) based on the FBI’s website. You can type in your own frequency order if you wish. When you click “Use Frequencies”, it will use the frequencies in the text field and generate a new key mapping (column on the far right of the page). Click “Decrypt” to use this mapping, and the plaintext field will be updated to contain your deciphered text. Your ***second option*** for decryption is to click the “Brute Force” method. This method will check every arithmetic offset of the base key “ABCDEFGHIJKLMNOPQRSTUVWXYZ” and keep track of the number of misspelled words. Ultimately, this functionality will choose the key with the lowest number of misspelled words, set this to be the key, and automatically decrypt the cyphertext into the plaintext field. You ***third option*** is to adjust the key yourself. The other two methods will not always yield perfect results, so you can modify the key mappings in the column on the far right of the page. Of course, once you’ve finished decrypting you can save the file by typing a filename into the “Filename to Save As:” text field then clicking the “Save Plain” button.

**Class Concepts**:

This project demonstrates the simple substitution cypher and how different techniques can be used to quickly decrypt messages that employ this cypher. Although it has been used since ancient times it remains relevant today. As reported in FBI publications, various forms of substitution cyphers are used by criminal organizations for record keeping and by prisoners who converse in letters with their associates.

One of the strengths of this project is that it reinforces two foundational concepts that apply to every form of encryption. The first is that any encryption which does not employ adequate diffusion is vulnerable to frequency cryptanalysis. The second is that any encryption which does not yield a sufficiently large set of possible outcomes is subject to brute force attack.

The design of the project was well suited to demonstrate these concepts while providing full functionality in an intuitive graphical interface.