CIS 4362 - Introduction to Cryptology

Final Project

Andrew Helms

12/09/20

Program

This program is an implementation of the ADFGVX cipher. It can encrypt the provided plaintext and decrypt the given ciphertext using the two provided keys. It uses the WINAPI to implement the GUI and uses simple textboxes and buttons for user input and output. The cipher implementation itself is done in separate files so they can be easily used in other programs. The encrypt and decrypt functions expect an input string, a Polybius Square key string, and a columnar transposition key string. All should be provided as strings from the standard library. The program will convert all characters to lowercase and strip any non-alphanumeric characters for the inputs. This makes the program fairly error resistant, as it will only throw an error if the input string or the columnar transposition key string don’t contain any valid characters. Then the cipher is executed and the resulting text, plaintext or ciphertext, is returned. For encryption, the Polybius Square substitution is done first, then the keyed columnar transposition. For decryption, the inverse of the keyed columnar transposition is done, then the inverse of the Polybius Square substitution. The last thing either function does is format the output into groups of 5 characters and put 10 of those groups per line.

Testing

Since the program is inherently error resistant, the number of test cases to be done is few. The first test I performed was providing the program random strings for the plaintext, the Polybius Square key, and the columnar transposition key. I then encrypted the message and immediately decrypted the resulting ciphertext to ensure that the decryption acts as the inverse of encryption. Next, I texted the algorithm to make sure it would correctly encrypt things based on known plaintext, ciphertext, and key combinations. I used the example provided in class as well as a few other examples found on the internet to perform this text. Lastly, I texted to ensure that the program would return the correct errors when invalid inputs were provided. To do this, I provided the program with empty inputs and non-empty inputs that only contained invalid characters. I did this test for both encryption and decryption. There are no known bugs.

References

These were the online references I used while researching for this project. This includes the websites visited for both implementation and cryptanalysis research.

<https://cryptography.fandom.com/wiki/ADFGVX_cipher>

<https://web.archive.org/web/20100503103848/http://www.vectorsite.net/ttcode_04.html#m3>

[<http://www.practicalcryptography.com/ciphers/adfgvx-cipher/>](http://www.practicalcryptography.com/ciphers/adfgvx-cipher/)

Links to the programming software packages used.

<https://docs.microsoft.com/en-us/windows/win32/apiindex/windows-api-list>

<https://visualstudio.microsoft.com/>