

**Assignment Answer**

**CSE432, Computer Security**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name: | Adham Nour | ID: | 1600226 |  |

Assignment No: ( 1 )

Date: 2 / 2 /2021

The Casear Cipher is declared “CaesarCipher,h” and implemented in “CaeserCipher.cpp”

If you want to use the Caeser Cipher, you can include the header file in the main function and invoke it by passing the plaintext and the key, the function would return you the ciphertext in form of string

The Same pattern applied to VigenereCipher

The Hill Cipher is implemented in the HillCipher class – which is implemented in the HillCipher.h file - ,but to use the hill cipher you should include the “HillCipherWrapper.hpp” instead, as it has one function “hill\_cipher” that wrap the details from the user. The “hill\_cipher” function takes two parameters which are the plaintext and the key. The HillCipher class is instanciated as static veriable to survive the function re-invokation (I mean instantiate it once and use it to the end of the program). Inside the HillCipher Class the vector “key” is stored to avoid any unnecessary vector copy for the same key.

The same pattern applied to PlayFair and Vernam Ciphers

attached to the file the executable for Linux (a.out), if windows machine is used, windows operating system now support running Linux program using WSL (Windows Subsystem for Linux)

to recompile and build the project in your machine using WSL or on Linux based machine the “runner.sh” shell script is provided to do so, that shell script is depending on “clang” that can be isntalled using “sudo apt install clang”.