Task 1. [25 points] Caesar's Cipher

1.1 Plain Text: APPLICATIONS OF CRYPTOGRAPHY AND CRYPTANALYSIS

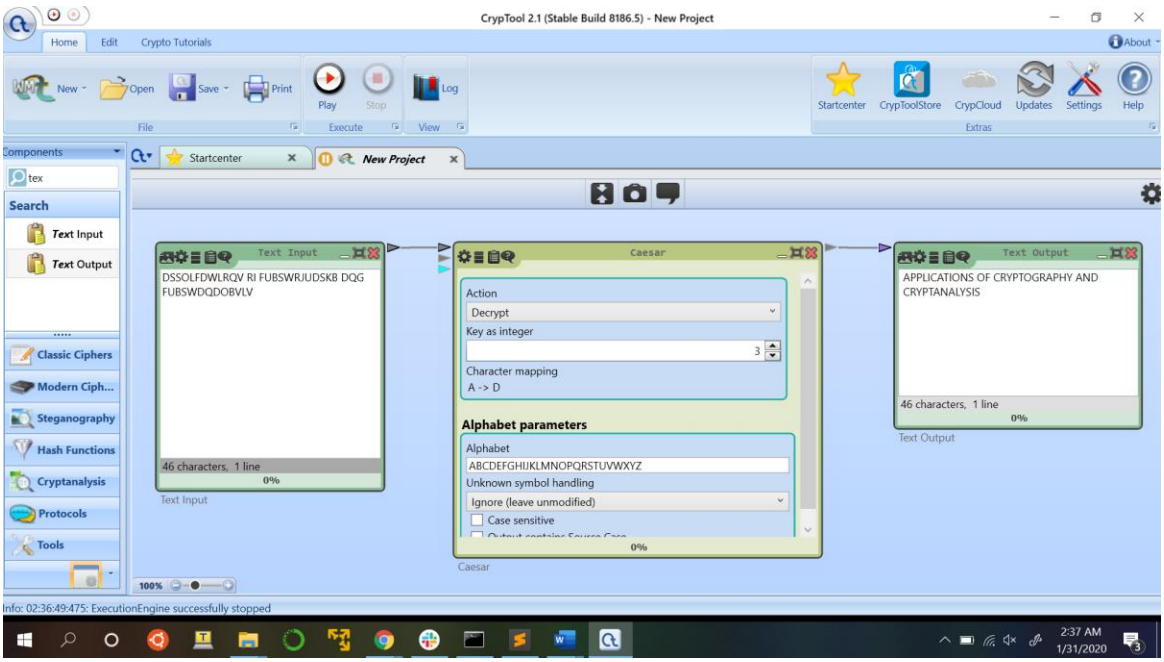

FIGURE 1.1: Screenshot for decryption process

1.2 Assuming that we choose K=13 as an encryption key in Caesar's cipher,

The result (Ci) of the following (double) encryption: Ci = E(K, E(K,Mi)) would be **plaintext**. Encrypting the plaintext twice with k=13 would result in loop around condition in case of ciphertext.

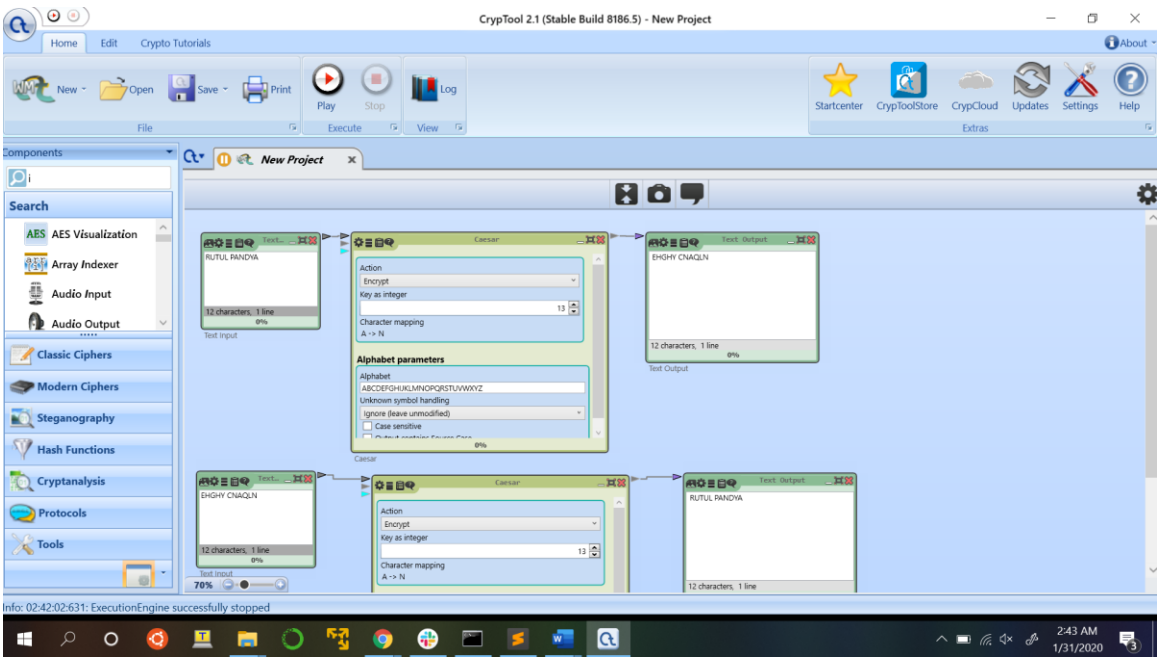

FIGURE 1.2: Screenshot for double decryption process with k=13

1.3 As there are 26 alphabets in English language, when we want to loop back to initial state, we need 13 times encryption with k=2 to get the same result as the previous one.

Task 2. [25 points] Frequency Analysis of the Caesar's Cipher

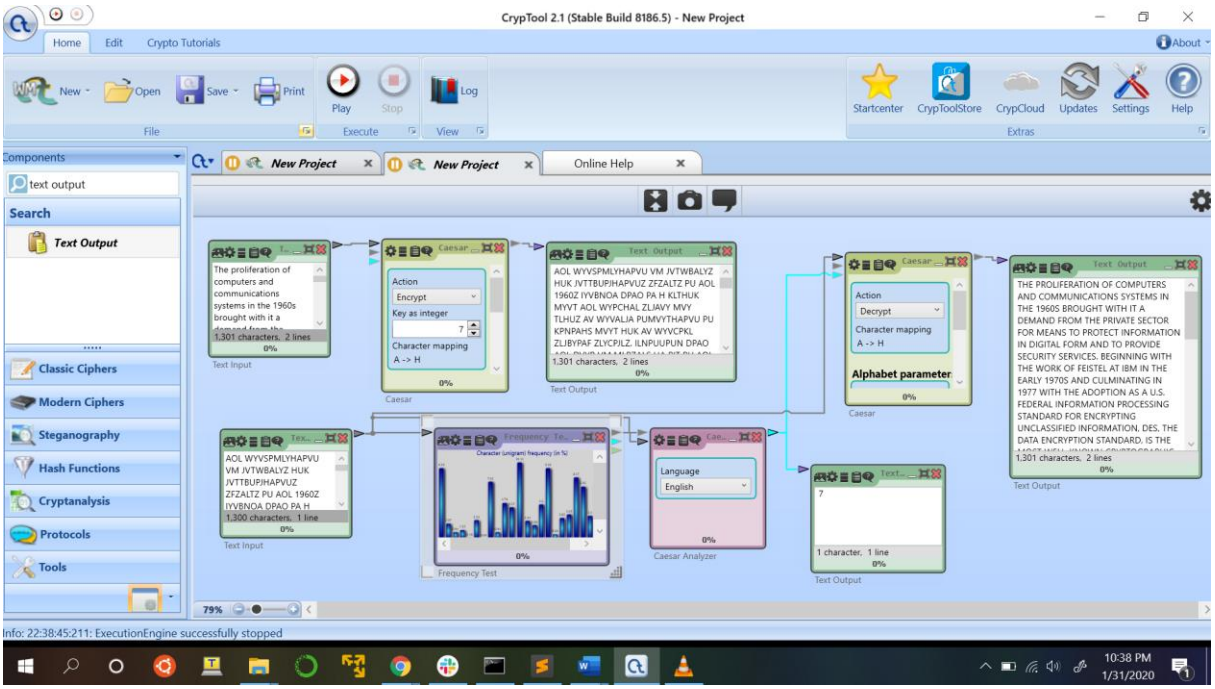

FIGURE 2.1: Screenshot for decrypting the Caesar's cipher using frequency analysis

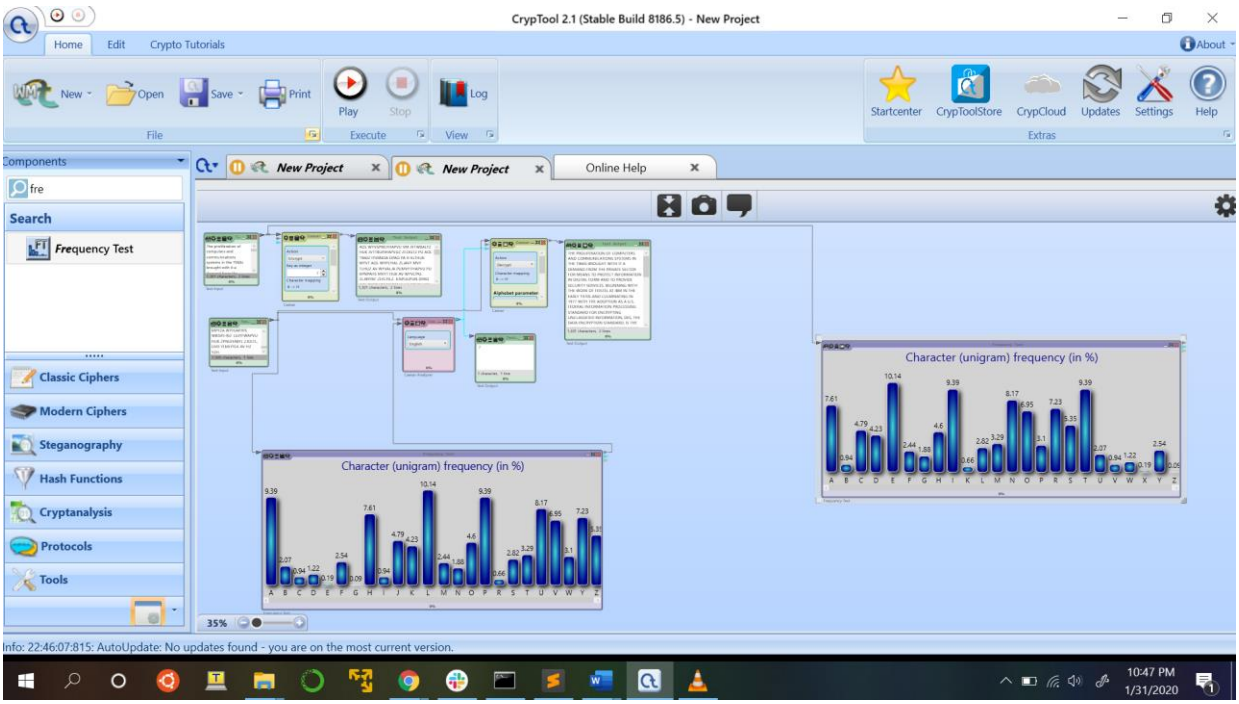

FIGURE 2.2: Screenshot for histograms of plaintext and of encrypted text of Caesar's cipher

Explanation:

Breaking Monoalphabetic Substitution Cipher by exploiting the frequency of alphabets in English language.

The methodology behind frequency analysis relies on the fact that in any language, each letter has its own personality. The most obvious trait that letters have is the frequency with which they appear in a language. Clearly in English the letter "Z" appears far less frequently than, say, "A". In times gone by, if you wanted to find out the frequencies of letters within a language, you had to find a large piece of text and count each frequency. Now, however, we have computers that can do the hard work for us. But in fact, we don't even need to do this step, as for most languages there are databases of the letter frequencies, which have been calculated by looking at millions of texts and are thus very highly accurate.

Task 3. [25 points] Monoalphabetic Substitution Cipher

Recovered Plain Text:

RECALL CAESAR'S CIPHER FALLS IN THE CATEGORY OF SUBSTITUTION MONOALPHABETIC CIPHERS I.E. EACH ELEMENT FROM THE PLAINTEXT WILL BE REPLACED WITH A UNIQUE ELEMENT FROM THE SPACE OF CIPHER TEXTS FOR THIS REASON A CIPEHERTEXT PRESERVES THE RELATIVE FREQUENCY AT WHICH PLAINTEXT ELEMENTS APPEAR IN THE CORRESPONDING PLAINTEXT. IN VERNAM CIPHER ENCRYPTION IS PERFORMED BY MEANS OF EXCLUSIVE OR XOR LOGICAL OPERATION PLAINTEXT IS XORED WITH AN ENCRYPTION KEY. IF AN ENCRYPTION KEY IS CHOSEN RANDOMLY AND IS AT LEAST AS LONG AS THE PLAINTEXT TO BE ENCRYPTED XOR ENCRYPTION ONE TIMEPAD IS PROVABLY PERFECTLY SECURE.

Key:

zyxwvutsr ponmlkjihgfedcb

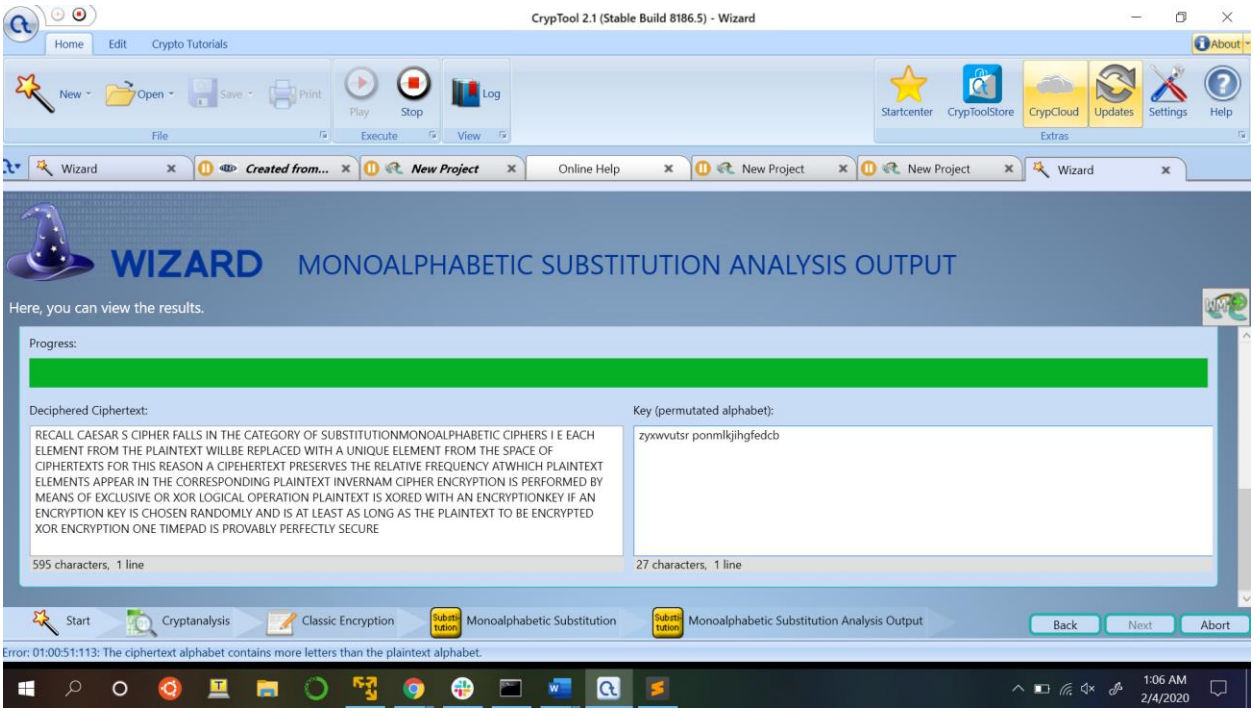

Figure 3.1: Screenshot of decrypted text obtained from cipher text using Monoalphabetic Substitution Analyzer.

Task 4. [25 points] Experiment with the template demos, including:

1. **Enigma**
2. **Vernam**
3. **Vigenère**

Plain Text: COMPUTER SECURITY IS IMPORTANT

Enigma Cipher

Key: CSCI

Cipher Text: KVTVNUXK DFHRCWGT GV PZNVOVCER

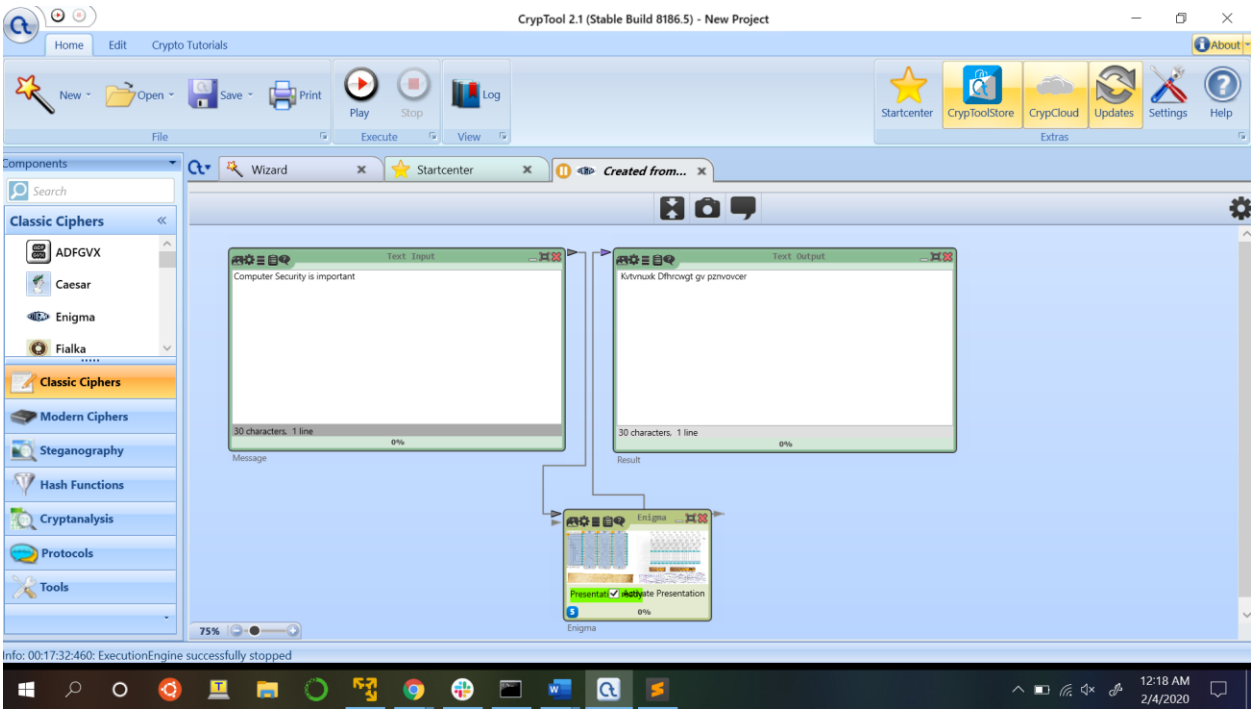

Figure 3.1: Screenshot of encryption using Enigma Cipher

Vernam Cipher

Cipher Text: egOXWlGZ KGKWjKba Ka aOXQjVIPl

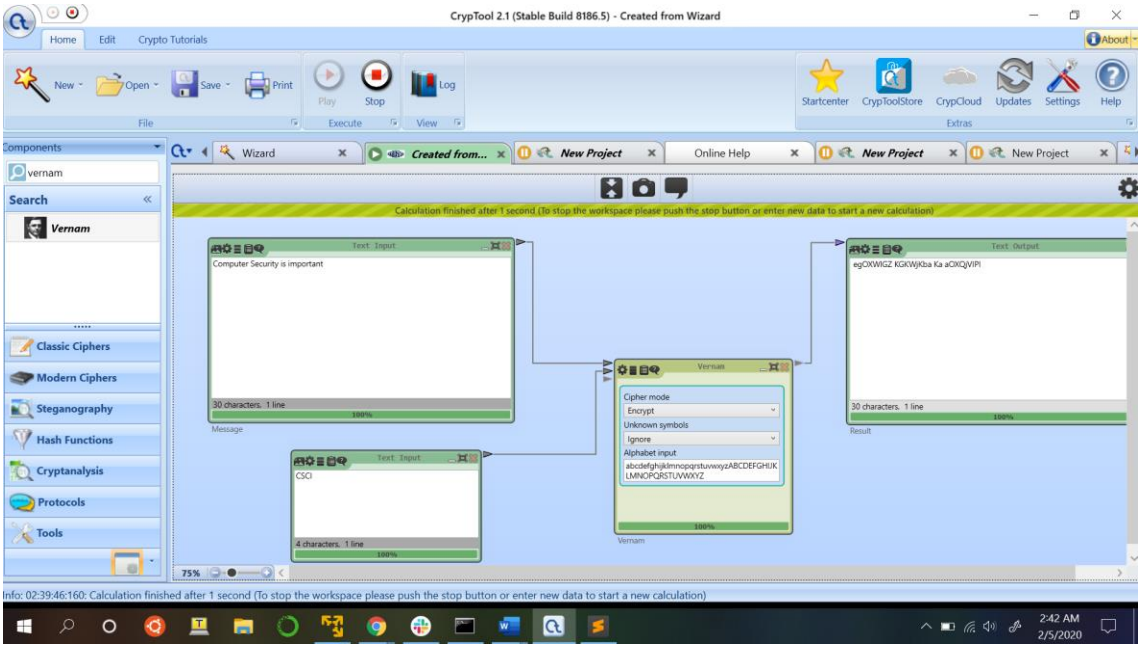

Figure 3.2: Screenshot of encryption using Vernam Cipher

Vigenère Cipher

Cipher Text: EGOXWLGZ UWECTAVG KK KURGTBCFV

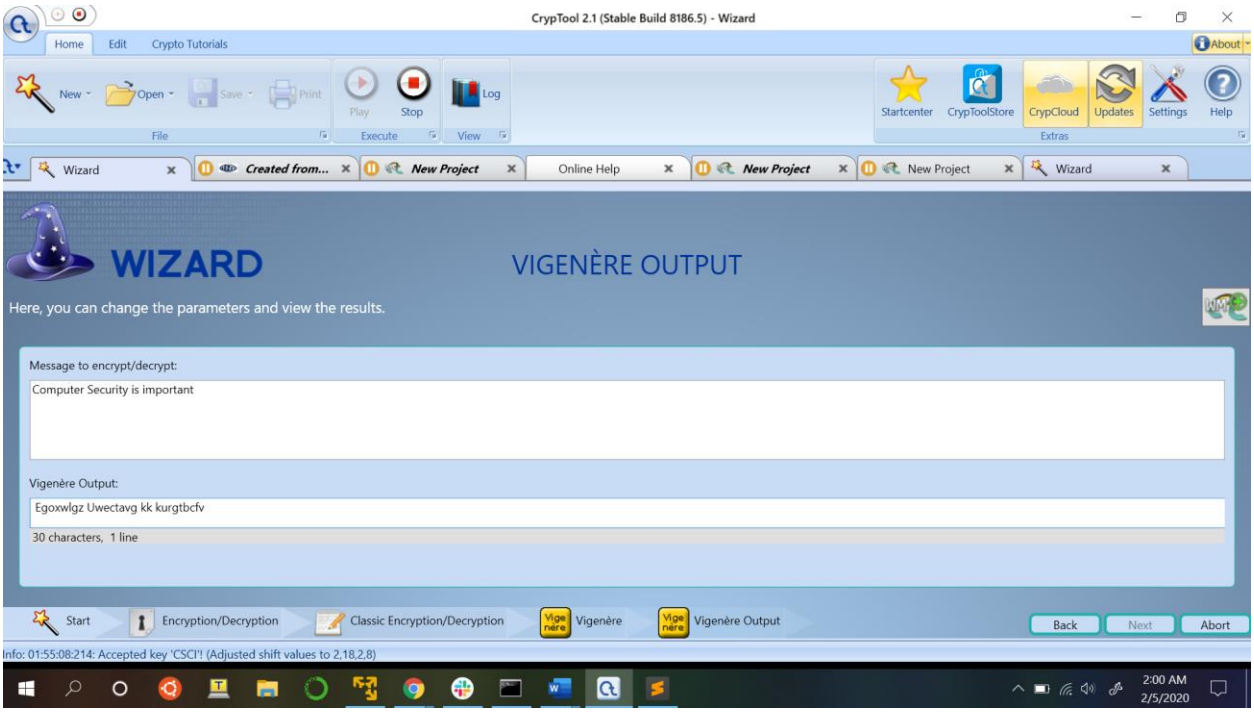

Figure 3.1: Screenshot of encryption using Vigenère Cipher