Attacks to Caesar Cipher

Learning Objectives: This exercise demonstrates an example of a brute-force attack cryptanalysis using frequency analysis.

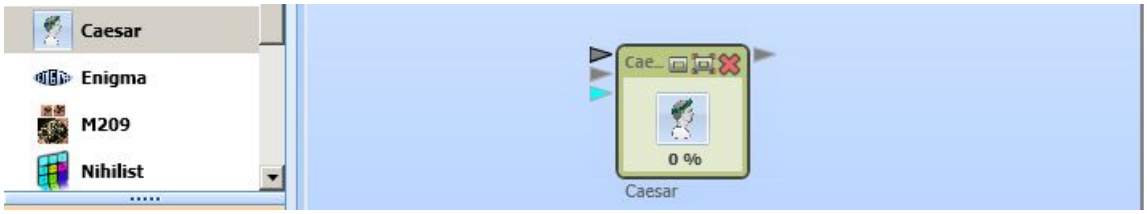
Summary: You will use CrypTool 2.0 for this exercise.

Deliverables: Submit a lab report by answering the review questions. In some review questions, you may provide screen captures.

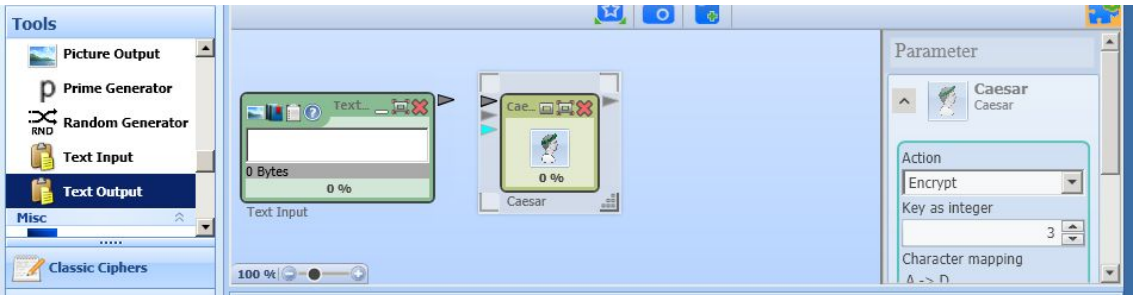
Brute-force attack

1. Start CrypTool 2.0 via the **Desktop Shortcut** or **Start menu**.
    a. (Start > Programs > CrypTool > CrypTool 2.0).
2. Under the **Home** tab, select new to create a new workspace.

3. From the **Classic Ciphers** tab, drag and drop the **Caesar Cipher** into the workspace.

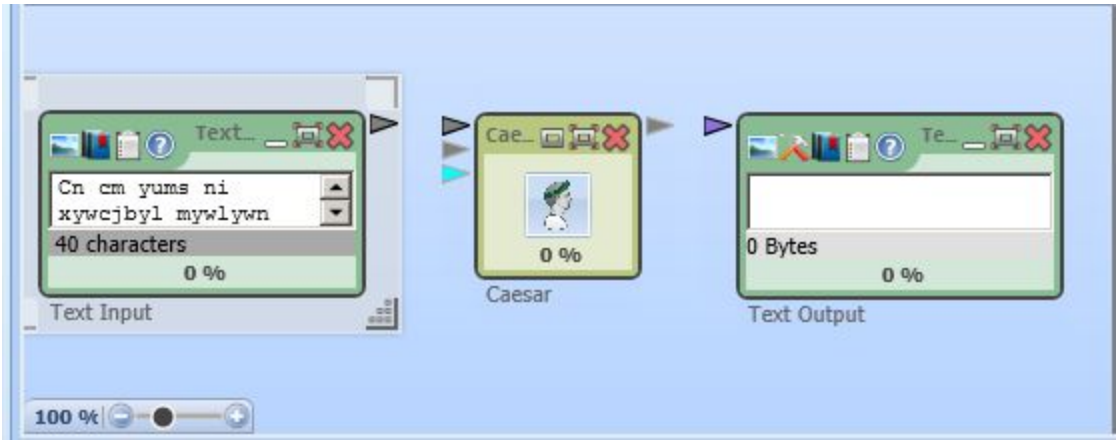


4. Next you will need to go into the **Tools** tab and scroll down until you see **Text Input** and **Text Output**. Drag and drop one of each into the workspace.

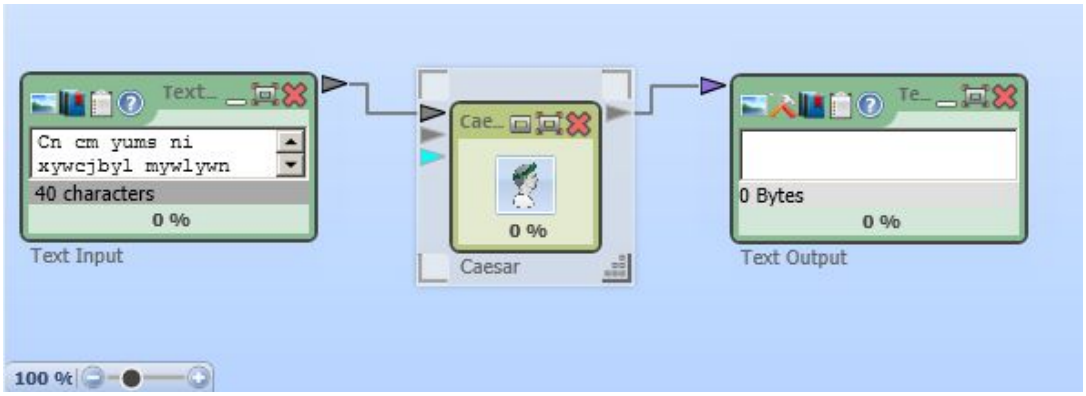


5. Copy the following ciphertext into the **Input Text** box. (You should able to copy and paste to the virtual computer)

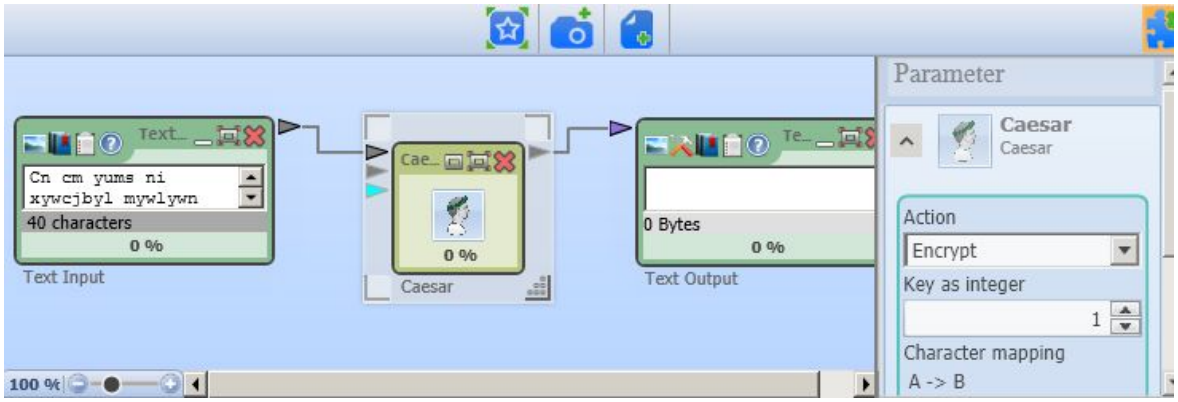
Cn cm yums ni xywcjbyl mywlyn gymmuaym!



6. Next you will need to link the **text boxes to the Caesar Cipher**. Click the arrow on the text input box and drag it to the arrow on the Caesar Cipher. Note that the **color of the arrows should match** when you connect them then click the arrow on right side of the Caesar Cipher and drag it to the arrow on the text output box.



7. Click on the **Caesar Cipher** box and under the Parameter menu, change **Action from Encrypt to Decrypt**. Then you will select **1 as your key to start**. Select Play to see the resulting Decryption. Keep changing the key until you find the secret message!



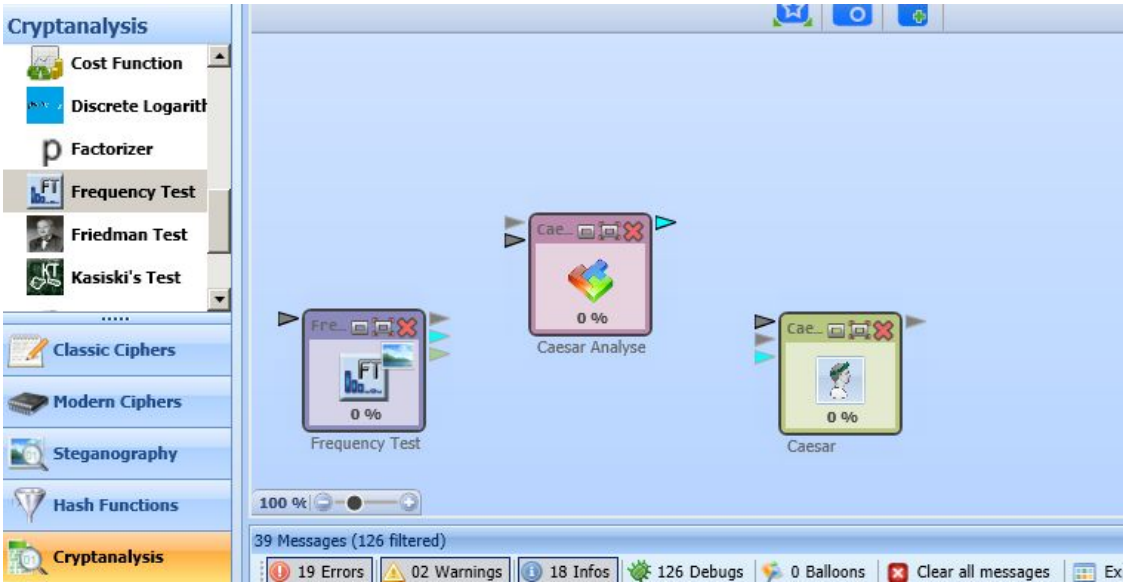
Review Questions (to be submitted)

- What is the secret message?
- What is the number of possible keys to try in the Caesar cipher?
- In order to perform a brute-force attack, what are the things that you need to know or have? In other word, what did enable you to use a brute-force attack in this case?

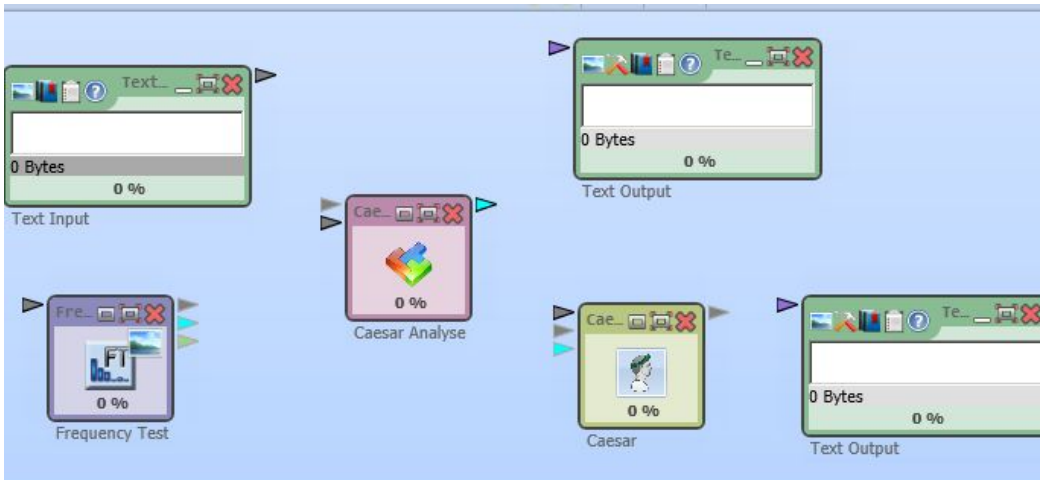
Frequency Analysis

In cryptanalysis, frequency analysis is the study of the frequency of letters or groups of letters in a ciphertext to aid to breaking traditional ciphers. In this exercise, you will use frequency analysis to decipher the ciphertext given below.

1. Start CrypTool 2.0 via the **Desktop Shortcut** or **Start menu**.
    a. It should already be opened.
2. First we will gather all the boxes needed to complete this activity. Start by dragging and dropping the **Caesar Cipher** into the work space.
3. Next you will select the **Cryptanalysis** row. Drag and Drop the **Caesar Analyser** box into the workspace. Scroll down to find the frequency test. Drag and Drop the **Frequency Test** into the workspace as well.



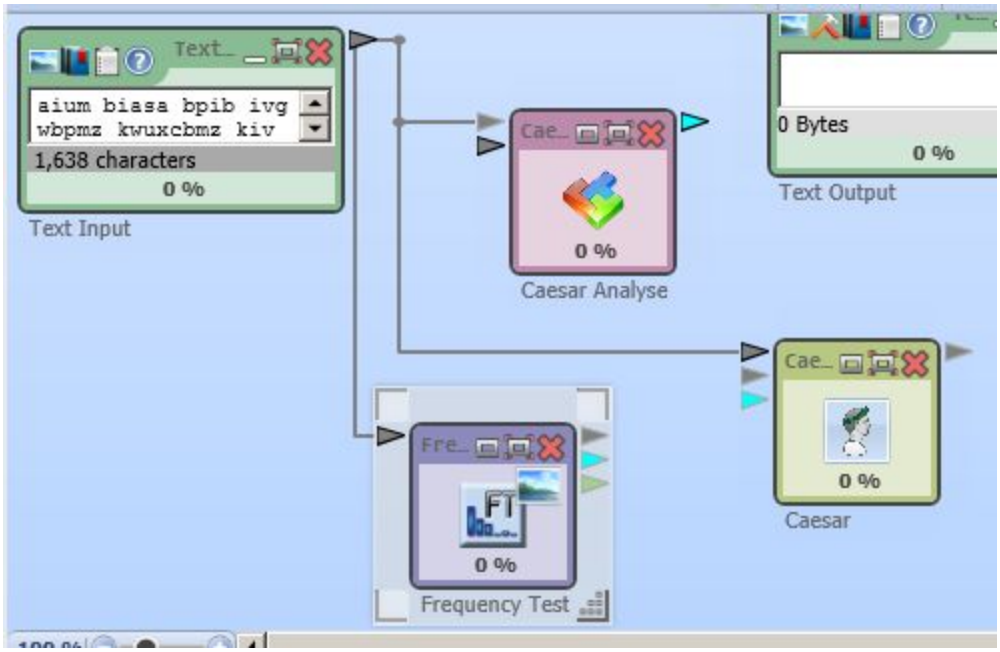
4. Now you should go to the **Tools** row and scroll down to the **text input** and **text output** boxes. You will need one text input box and two text output boxes. Drag and drop them into the workspace. It should look similar to the image below.



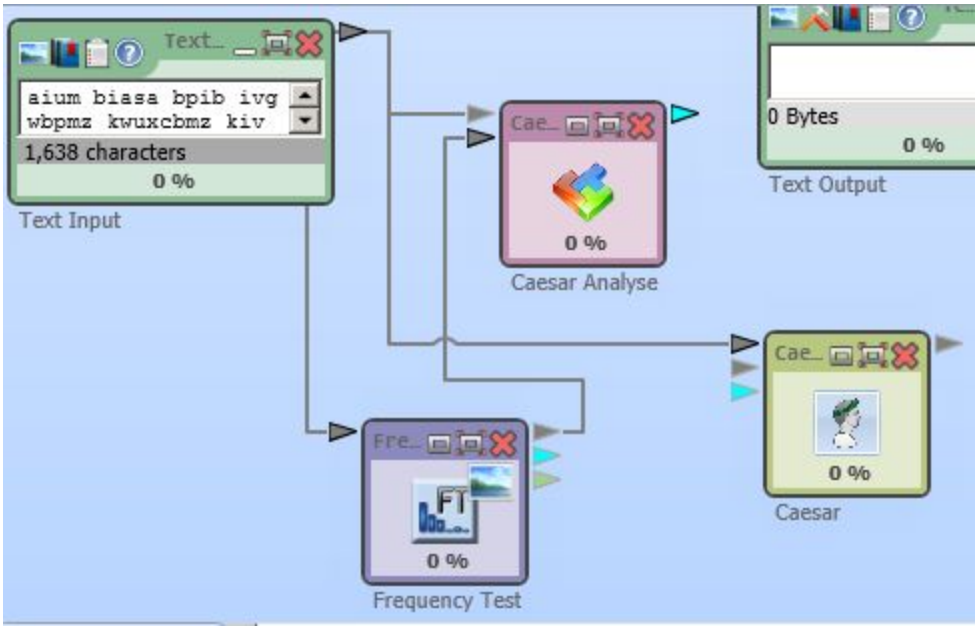
5. Copy the ciphertext given below and paste it into the text input box.

I kwuxcbmz qa i uikpqvm bpib uivqxctibma libi ikkwzlqvo bw i tqab wn qvabzckbqwva. Bpm nqzab lmdqkma bpib zmamujtm uwlmzv kwuxcbmza libm bw bpm uql-bemvbqmbp kmvbczg, itbpwcop bpm kwuxcbmz kwvkmxb ivl dizqwca uikpqvma aquqtiz bw kwuxcbmza mfqabml miztqmz. Miztg mtmkbzwvqk kwuxcbmza emzm bpm aqhm wn i tizom zwwu, kwvacuqvo ia uckp xwemz ia amdmzit pcvlzml uwlmzv xmzawvit kwuxcbmza. Uwlmzv kwuxcbmza izm jiaml wv bqvg qvbmozibml kqzkcqba ivl izm uqttqwva bw jqttqwva wn bquma uwzm kixijtm epqtm wkkcxgqvo i nzikbqwv wn bpm axikm. Bwlig, aquxtm kwuxcbmza uig jm uilm auitt mvwcop bw nqb qvbw i ezqabeibkp ivl jm xwemzml nzwu i eibkp jibbmzg. Xmzawvit kwuxcbmza, qv dizqwca nwzua, izm qkwva wn bpm Qvnwzuibqwv Iom ivl izm epib uwab xmwxtm bpqvs wn ia “i kwuxcbmz”; pwemdmz, bpm uwab kwuuwv nwzu wn kwuxcbmz qv cam bwlig qa bpm mujmllml kwuxcbmz. Mujmllml kwuxcbmza izm auitt, aquxtm lmdqkma bpib izm caml bw kwvbzwt wbpmz lmdqkma — nwz mfiuxtm, bpmg uig jm nwcvl qv uikpqvma zivoqvo nzwu nqopbmz iqzkzinb bw qvlcabzqit zwjwba, lqoqbit kiumzia, ivl kpqtlzmv'a bwga. Bpm ijqtqbg bw abwzm ivl mfmkcbm tqaba wn qvabzckbqwva kittml xzwoziua uisma kwuxcbmza mfbzmumtg dmzaibqtm ivl lqabqvocqapma bpmu nzwu kitkctibwza. Bpm Kpczkp–Bczqvo bpmaqa qa i uibpmuibqkit abibmumvb wn bpqa dmzaibqtqbg: ivg kwuxcbmz eqbp i kmzbiqv uqvqucu kixijqtqbg qa, qv xzqvkqxtm, kixijtm wn xmznwzuqvo bpm aium biasa bpib ivg wbpmz kwuxcbmz kiv xmznwzu. Bpmzmnwzm, kwuxcbmza eqbp kixijqtqbg ivl kwuxtmfqbg zivoqvo nzwu bpib wn i xmzawvit lqoqbit iaaqabivb bw i acxmzkwuxcbmz izm itt ijtm bw xmznwzu bpm aium kwuxcbibqwvit biasa oqdmv mvwcop bqum ivl abwziom kixikqbg.

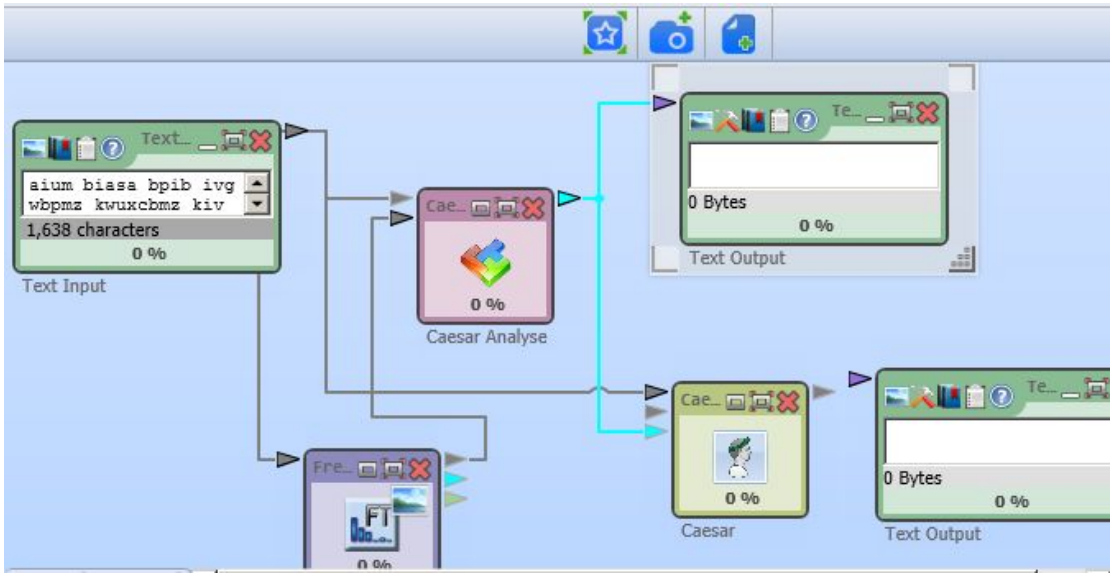
6. Now that we are prepared, we can begin connecting the boxes. Some arrows/boxes will be connected to multiple boxes this time. The **text input** box will need to be connected to the **Caesar Analyser, Frequency Test, and Caesar Cipher** boxes.



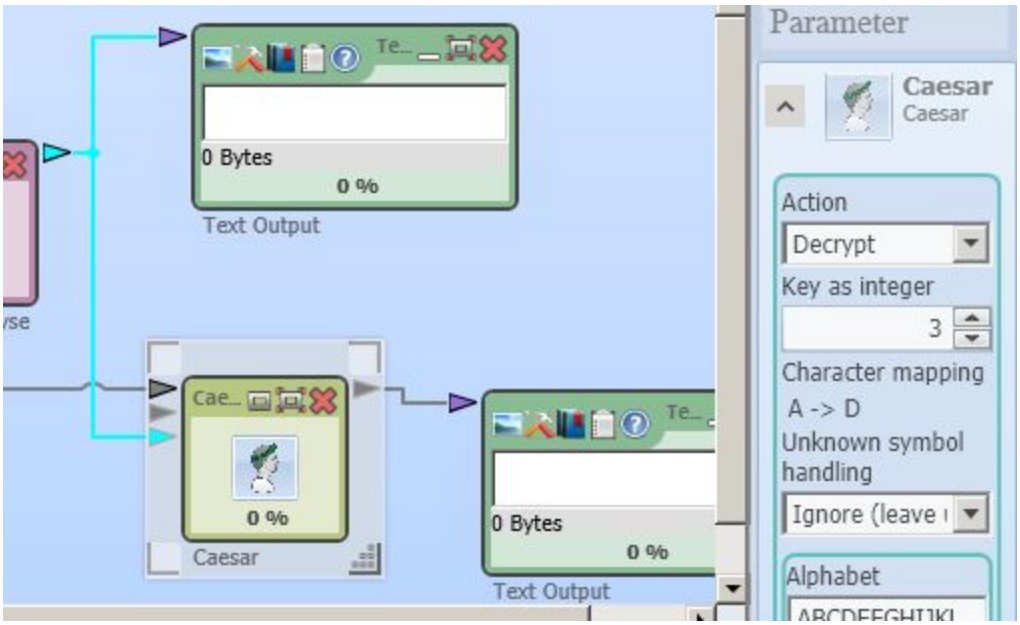
7. Next you will connect the **Frequency Test** to the **Second left arrow** on the **Caesar Analyser** box.



8. Connect the **Caesar Analyser** (right arrow) to the **first text output box** and the **blue arrow on the Caesar Cipher Box**. It should look similar to the image below.



9. Now you need to connect the **Caesar Cipher** to the **Second Text box**. You will also need to make sure that the **Caesar Cipher** is set up for **Decryption** under the Parameter box.



10. Once the boxes are connected and the Caesar Cipher is ready for Decryption, Press Play to see the results. Please answer the questions below.

Review Questions (to be submitted)

- What is the key?
- Was the ciphertext deciphered correctly? What is the first three words of the plaintext.
- Explain how the CrypTool was able to decrypt the ciphertext by using the frequency of the letters.
- Try the following for Vinegere Cipher. Encrypt the plaintext that you just deciphered using the Vinegere Cipher as follows. Go to Encrypt/Decrypy > Symmetric Classic > Vinegere and use REDFLAG as the key to encrypt the plaintext. Then, go to go to Analysis > Symmetric Encryption (classic) > Cihertext Only > Vinegere. Can you recover the key and decrypt the message correctly?