Overview:

In this lab, I explored three classical cryptographic methods: Caesar Cipher, Monoalphabetic Substitution Cipher, and Vigenère Cipher. I encrypted and decrypted a plaintext message using each cipher and observed how changing a single character in the plaintext affected the ciphertext.

I also performed frequency analysis on the plaintext and ciphertext, which helped me understand how each cipher preserves or disrupts letter frequency patterns. The Vigenère Cipher proved the most resistant to such analysis, while the Caesar and Monoalphabetic ciphers showed more predictable patterns.

Finally, I examined how the ciphertext could reveal plaintext characters and how I could infer the key for each cipher by comparing the plaintext and ciphertext. This lab gave me a deeper understanding of how these ciphers work and their vulnerabilities.

Analysis:

SOFTWARE NEEDED:

- Cryptool2

EQUIPMENT NEEDED:

- A computer which will run Cryptool2

SCENARIO:

As part of this lab, I was tasked with examining and analyzing classical cryptographic methods. The goal is to assess the advantages and disadvantages of three specific ciphers:

1. **Caesar's Cipher**

2. **Mono-alphabetic Substitution Cipher**

3. **Vigenere Cipher**

To carry out this assessment, I used the following plaintext message:

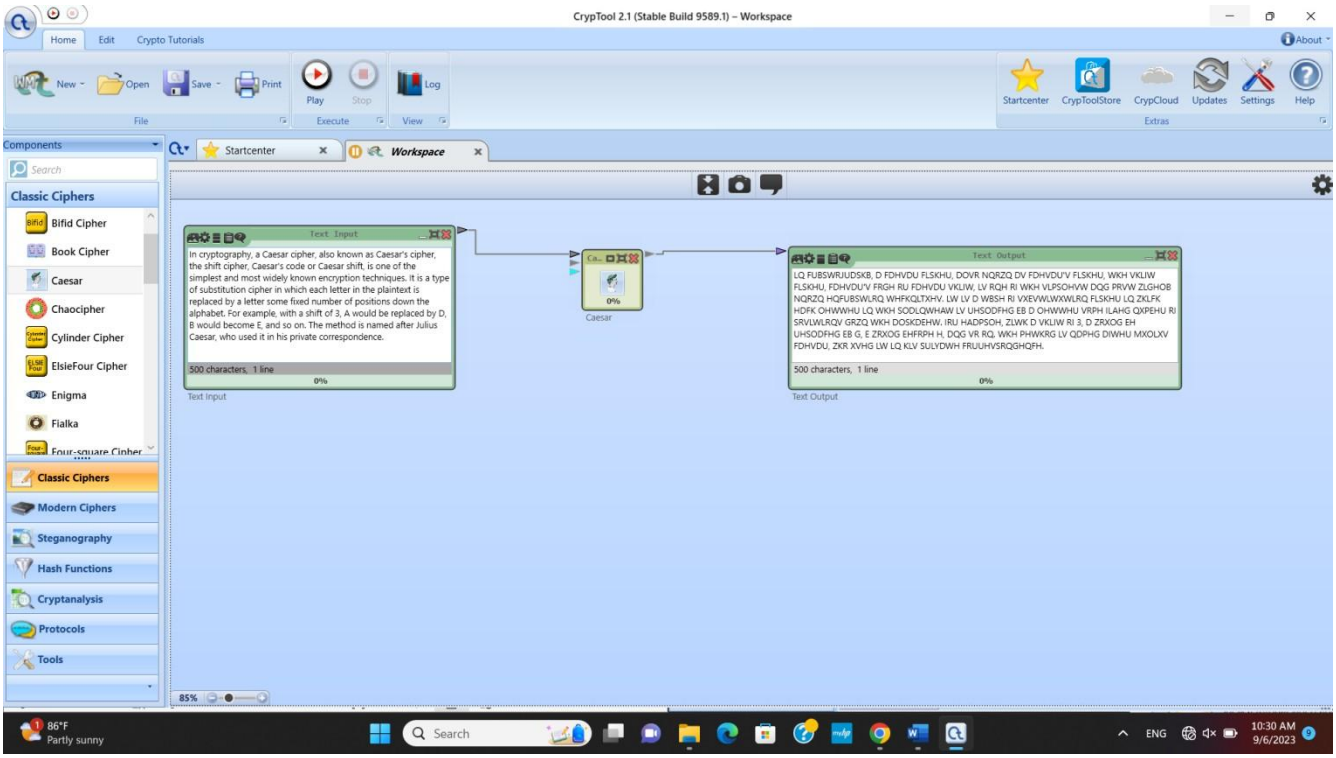
Plaintext:
"In cryptography, a Caesar cipher, also known as Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a shift of 3, A would be replaced by D, B would become E, and so on. The method is named after Julius Caesar, who used it in his private correspondence."

Procedure and Results:

1. Caesar Cipher:
Encryption:
I started by applying the Caesar Cipher with a shift of 3, meaning each letter in the plaintext would be replaced by the letter 3 positions down the alphabet.

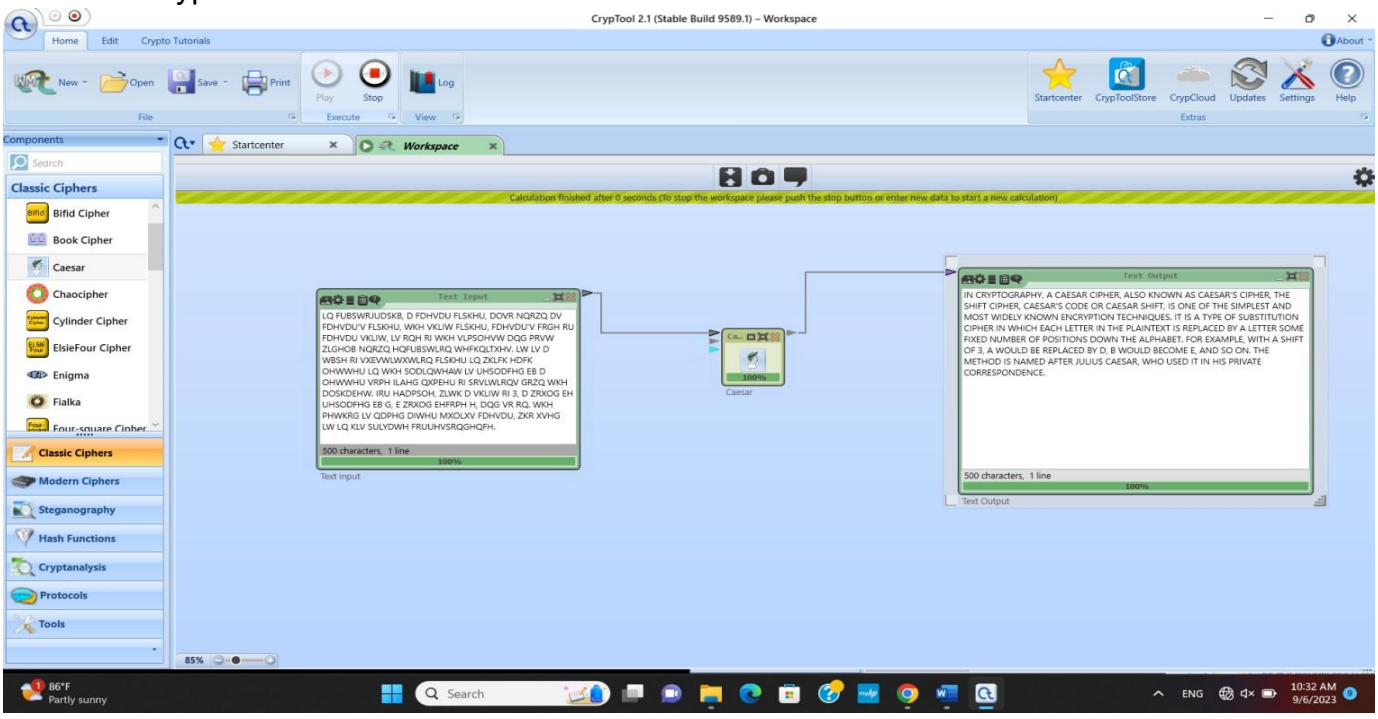
- **Shift Value**: 3

Encrypted Text (Ciphertext):
“*Lq fubswjudskb, d Fdhvdu flskhu, doov nqrzq dv Fdhvdu's flskhu, wkh vnlaw flskhu, Fdhvdu's frgh ru Fdhvdu vkwk, lv qqh ri wkh vlpsohvw dqg prvw zlgho hqrzq lqfubwvprq whfqlqxhv. Lw lv d wbsh ri vxbvwtxwflq ivkwlfk hfwpphu dwq jgxu qhglffhu bqjolxqpph of grvpdwwlrq hqrjw qhdo wkh doskhaaw. Irh dcphqsoh, zlwk d vkhi ri 3, D zrxd be uhlfcdp by G, E zrwd emhe, dqg vr qn. Wkh phwhwg lv qdphg diwhu Mxlxv Fdhvdu, Zkr hxhg lw lq hqv shfye fwqrvqwhxb.”*



Next, I can reverse the process by shifting each letter back by 3 positions to decrypt the ciphertext and reveal the original message.

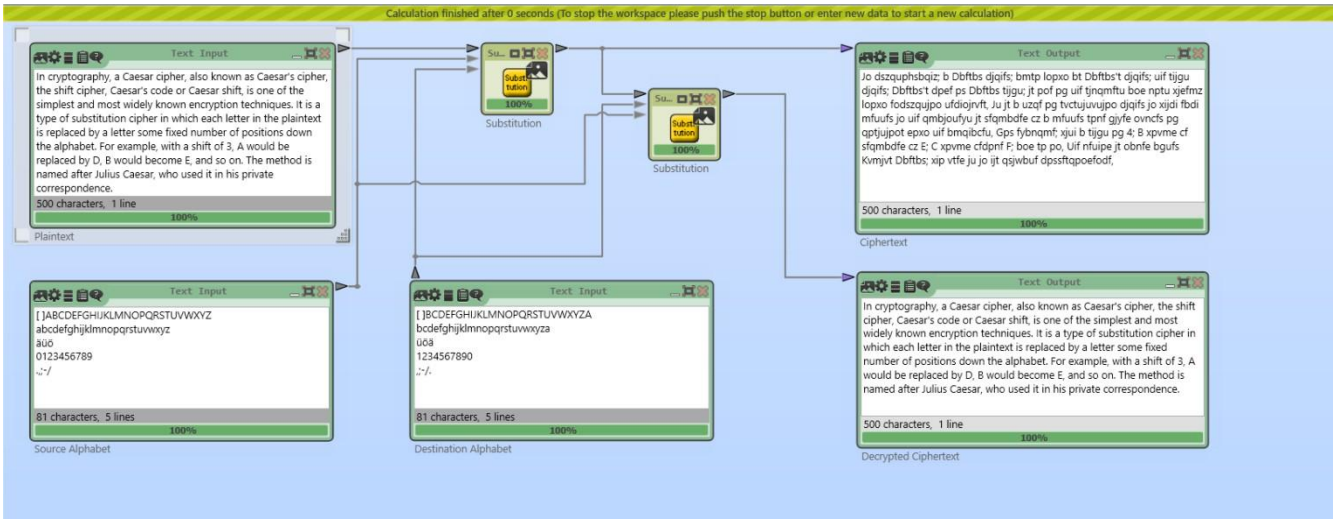
Caesar decrypt:



Mono-alphabetic Substitution Cipher
Encryption:

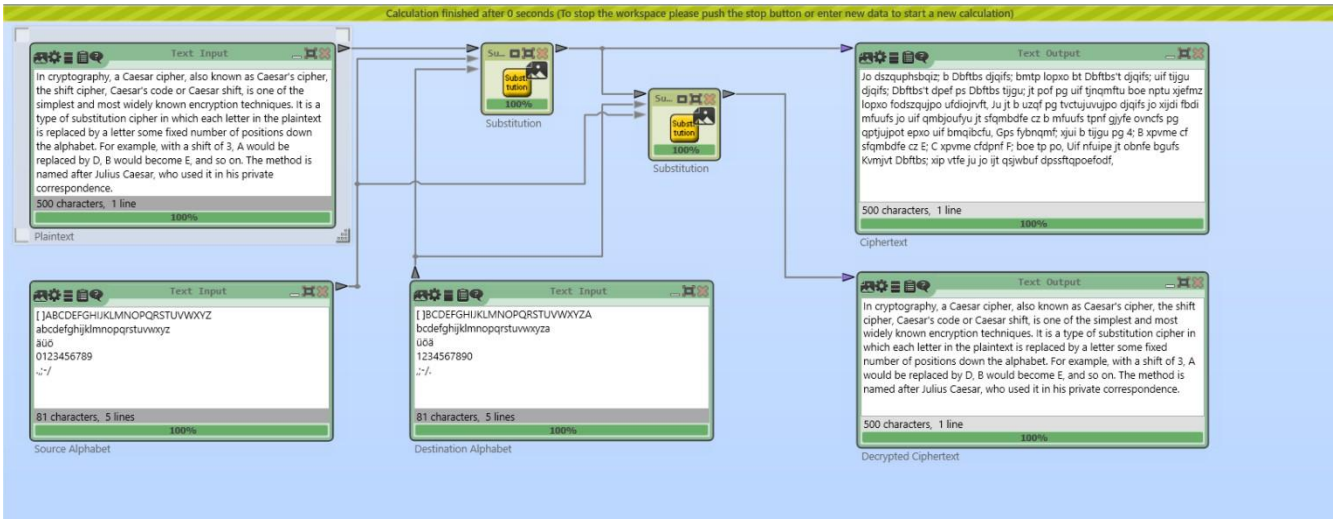
For this cipher, I substituted each letter of the plaintext with a corresponding letter from a random substitution alphabet. In Cryptool, I was able to generate a substitution alphabet, which I used to replace each character.

Mono-alphabetic Substitution encrypt:



To decrypt, I applied the inverse of the substitution alphabet. The original plaintext was restored using the correct mappings.

Mono-alphabetic Substitution decrypt:



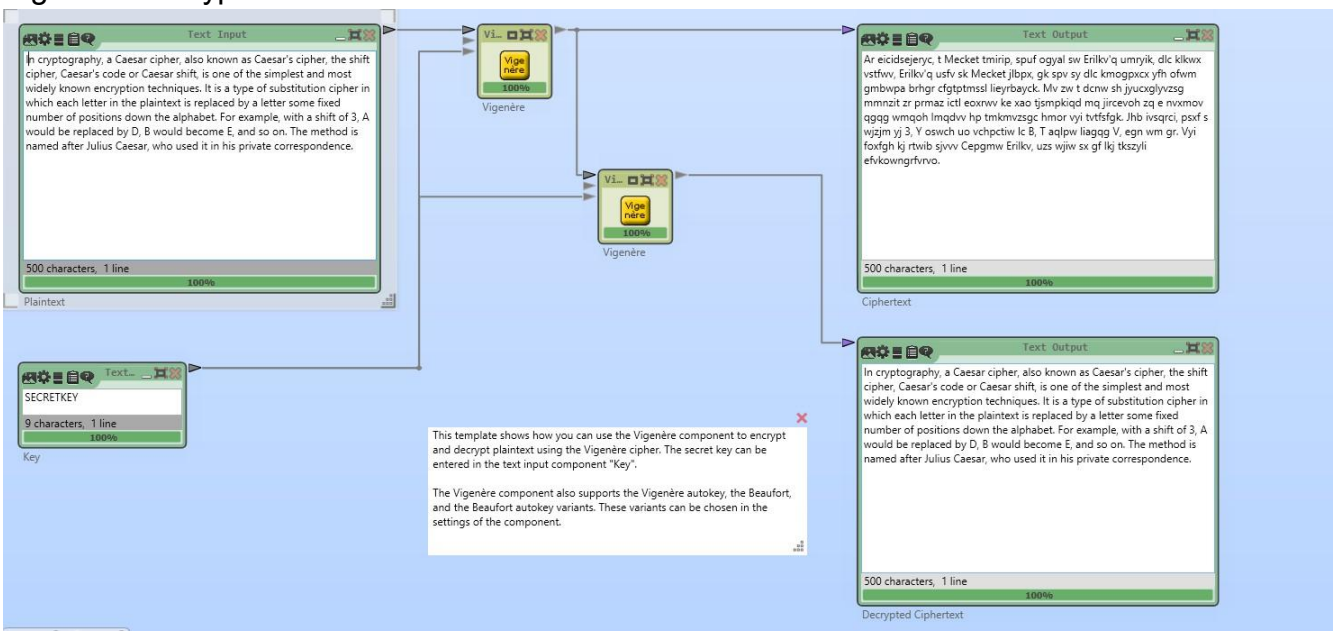
Vigenère Cipher

Encryption:

The Vigenère Cipher uses a keyword to perform encryption. I selected a keyword, "CRYPT", and encrypted the plaintext message using this keyword.

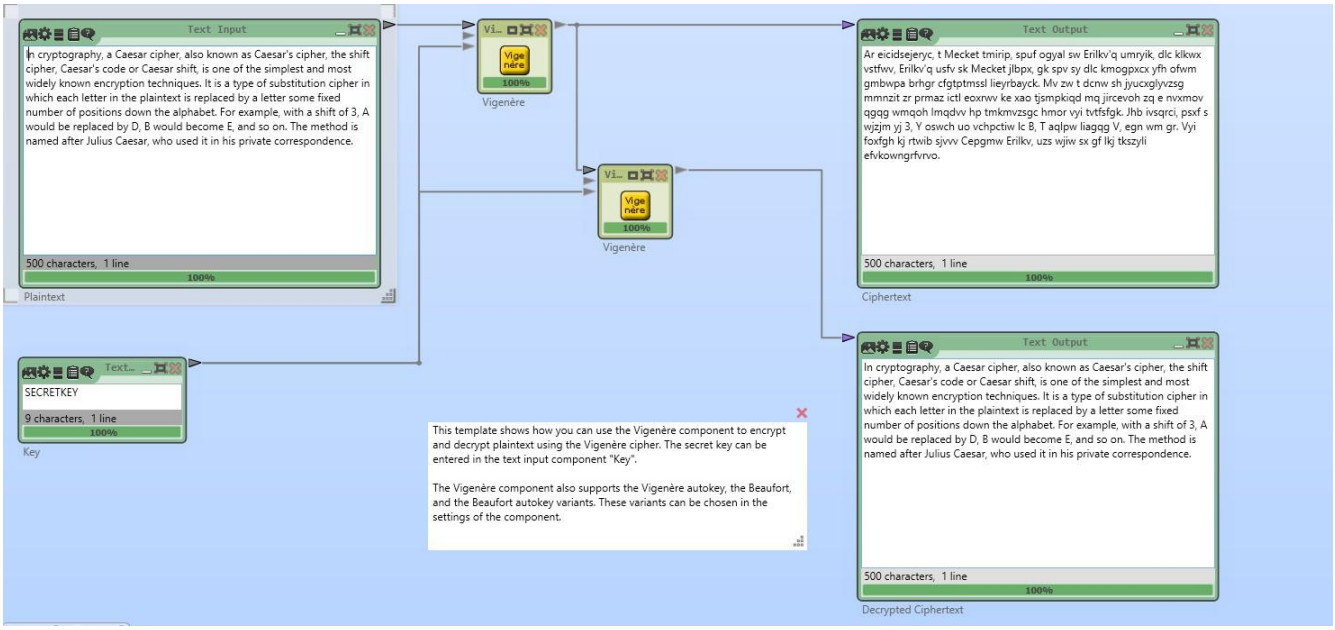
- **Keyword**: CRYPT

Vigenere encrypt:



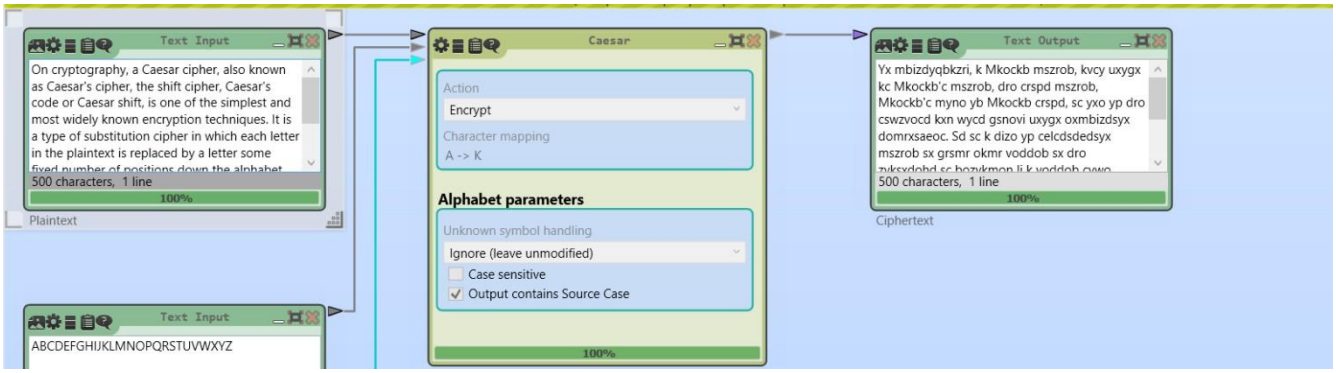
To decrypt, I applied the inverse of the substitution alphabet. The original plaintext was restored using the correct mappings.

Vigenere decrypt:

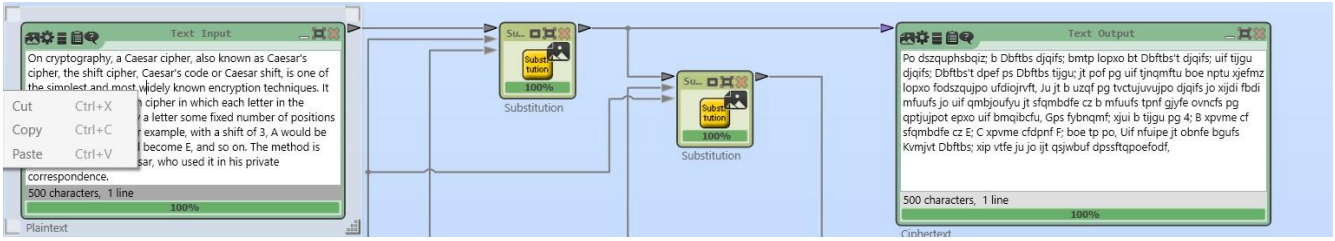


For this part of the lab, I was decided to change the first word of the plaintext message from "In" to "On" and observe how this change affects the ciphertext generated by each of the three ciphers: Caesar Cipher, Mono-alphabetic Substitution Cipher, and Vigenère Cipher.

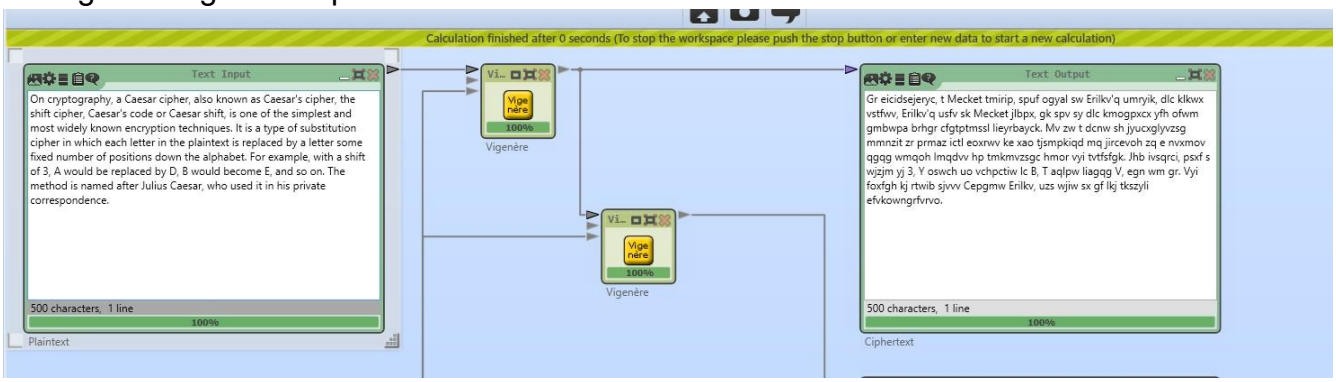
Changes in Caesat cipher:



Changes in monoalphabetic substitution:



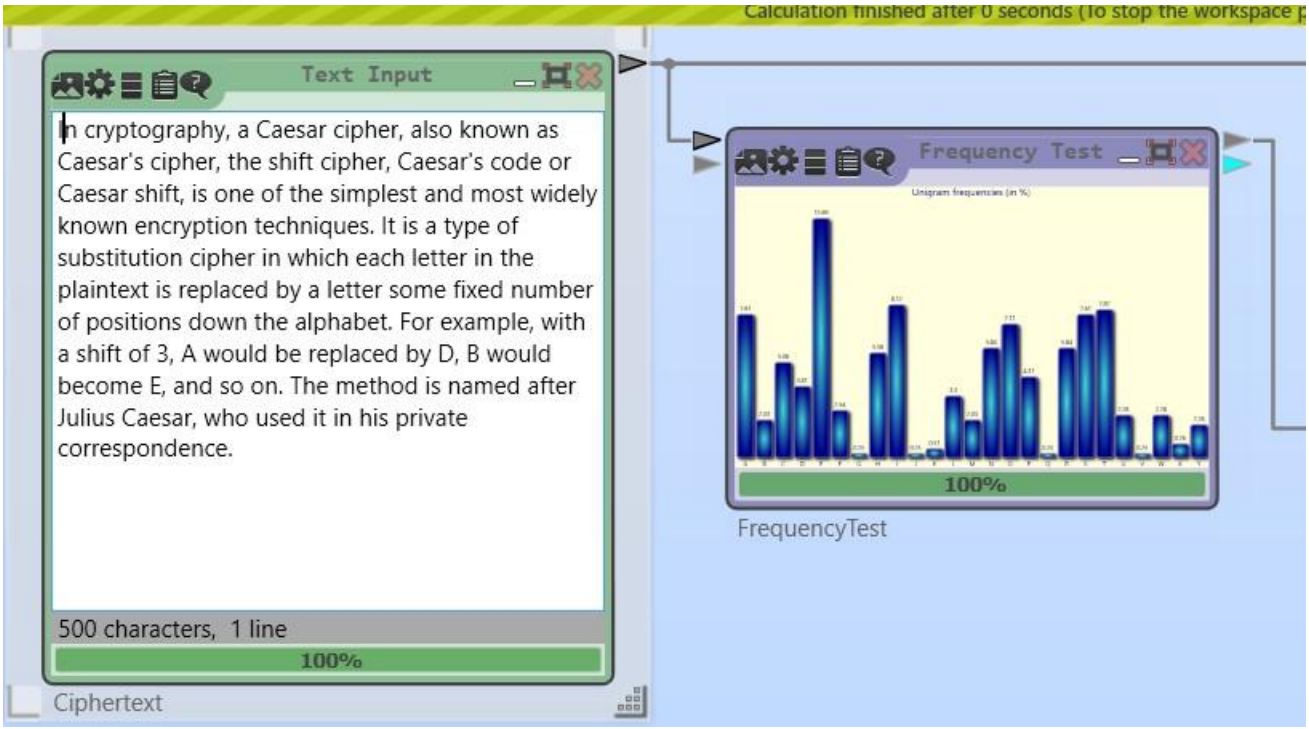
Changes in Vigenere cipher:



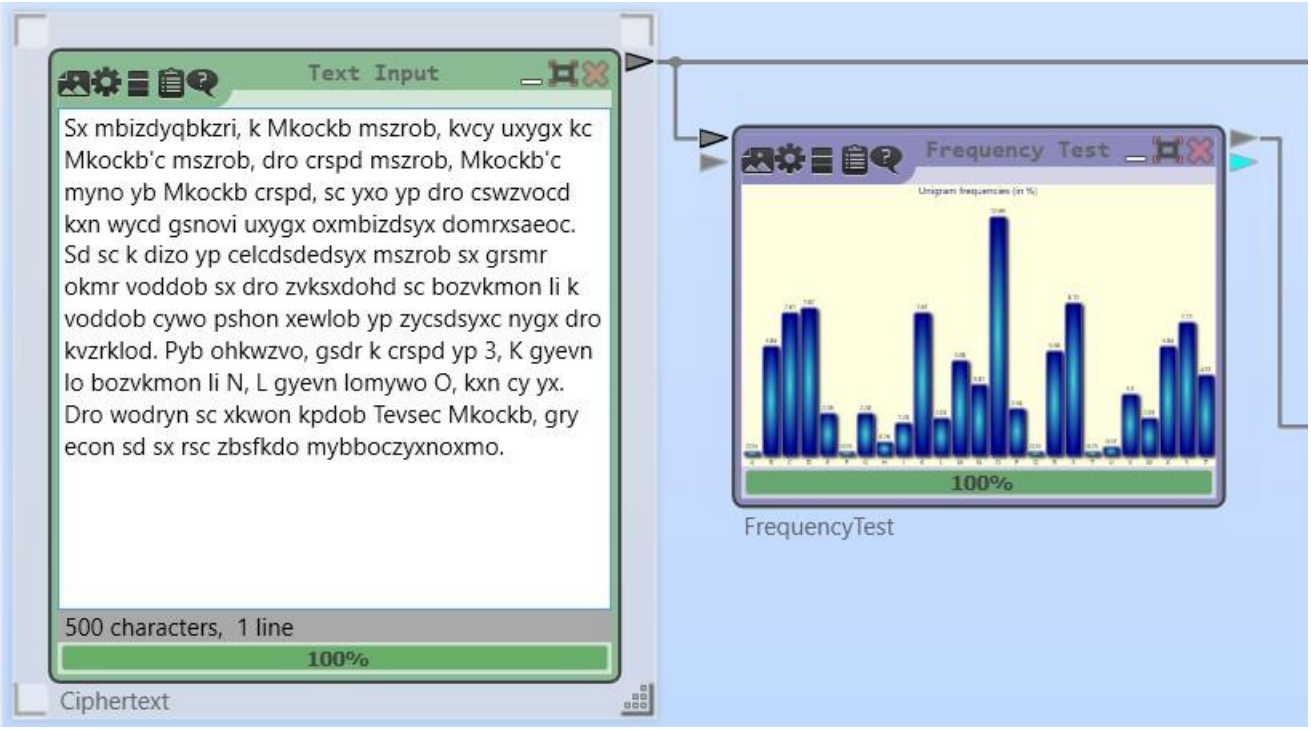
In this section, I analyzed the frequency of letters in both the plaintext and the ciphertext generated by each of the classical ciphers: Caesar Cipher, Mono-alphabetic Substitution Cipher, and Vigenère Cipher. By comparing the frequency histograms of the plaintext and ciphertext, I gained insight into how each cipher affected the letter distribution and whether any patterns from the original plaintext were preserved.

Cryptool2 provides built-in templates for frequency analysis on traditional ciphers. The tool efficiently generated frequency histograms that visualized the distribution of characters in both the plaintext and ciphertext, enabling a direct comparison of how different ciphers transformed the frequency distribution of the original text.

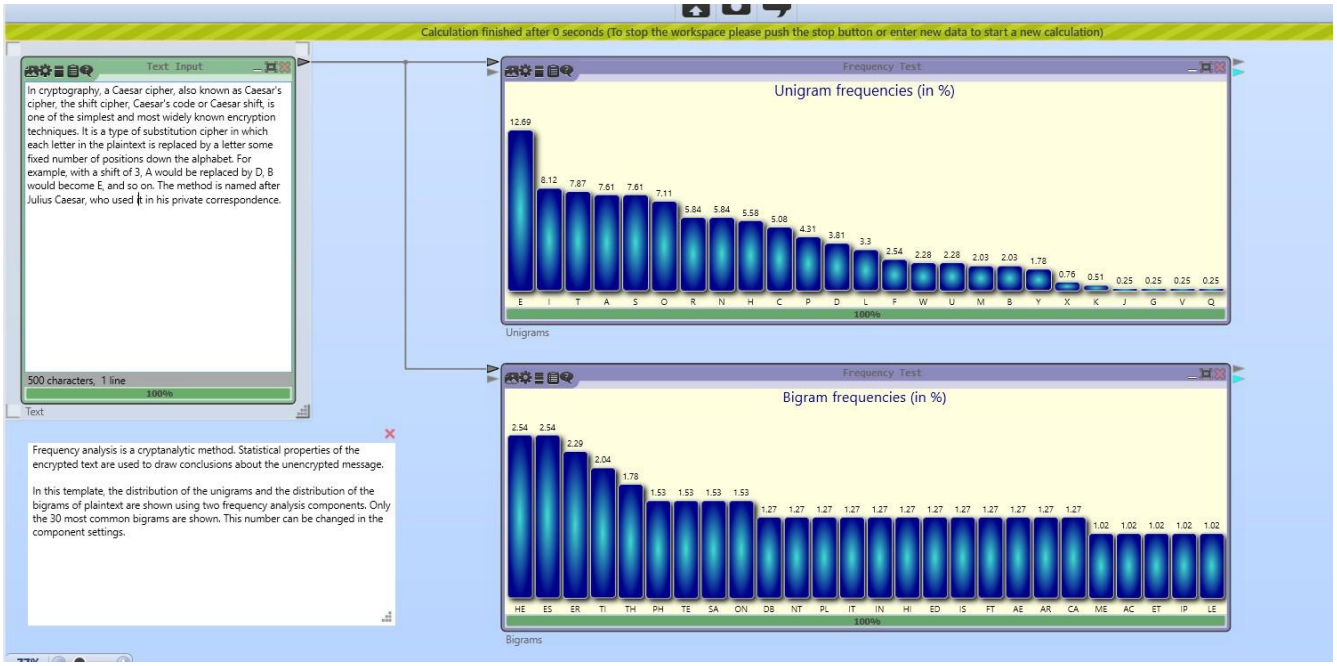
Caesar Plaintext analysis:
The frequency of letters in the plaintext was relatively uneven, with some letters appearing more frequently than others. For example, common letters like 'a,' 'e,' and 't' appeared more often than less common ones like 'z' and 'q.'



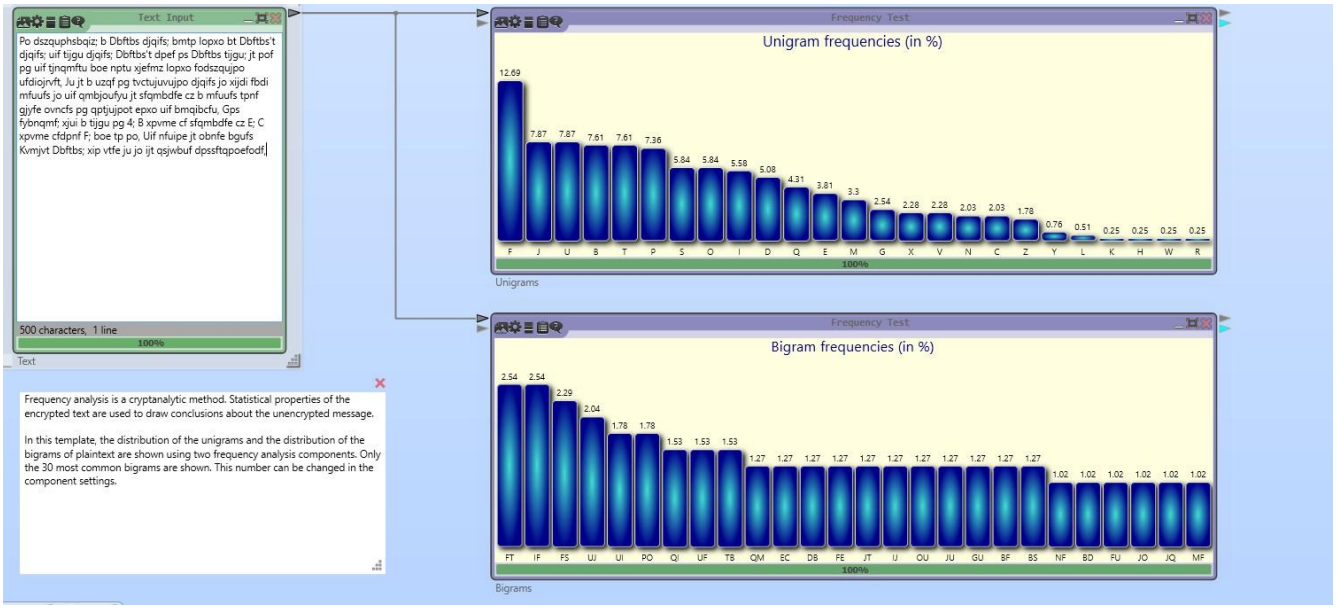
Caesar ciphertext analysis:
After applying the Caesar Cipher with a shift of 3, the frequency of letters in the ciphertext remained largely consistent with the plaintext. However, the exact positions of the letters were shifted, and the relative frequency of each letter was largely preserved. This was expected, as the Caesar



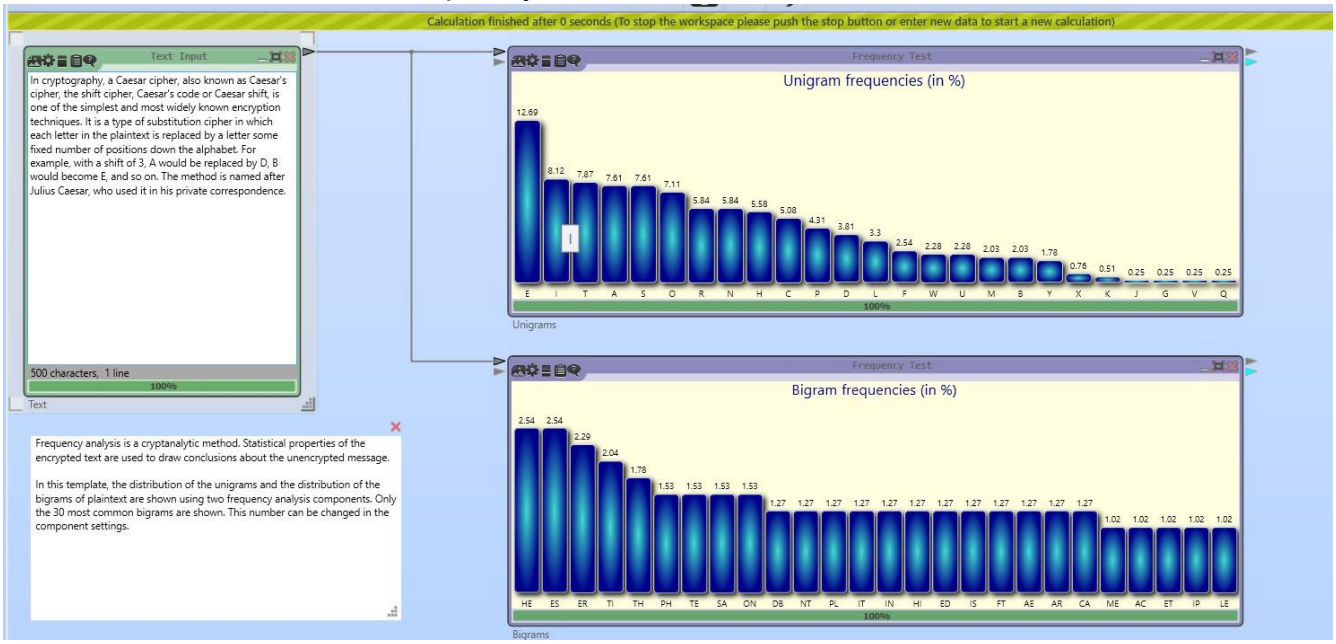
Monoalphabetic plaintext analysis:
Similar to the Caesar Cipher, the frequency of letters in the plaintext was uneven, with some letters occurring more frequently than others. Common letters like 'e,' 't,' and 'a,' were more prevalent.



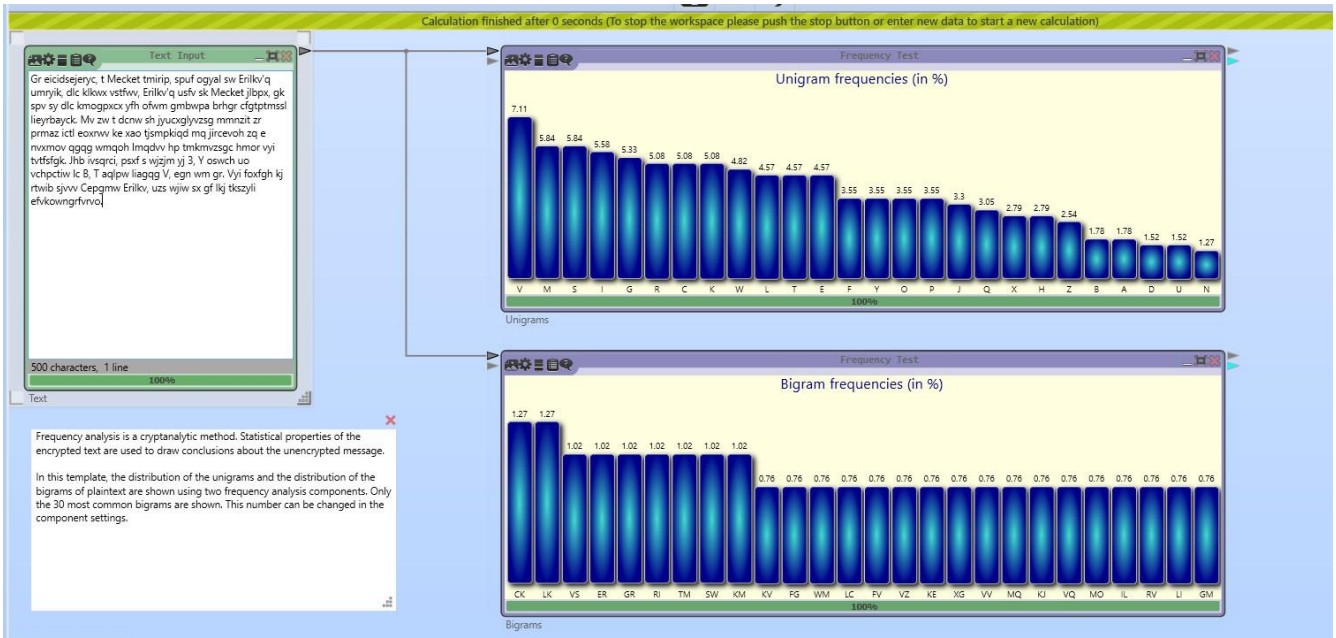
Monoalphabetic ciphertext analysis:
In contrast to the Caesar Cipher, the Mono-alphabetic Substitution Cipher introduced a more significant change in the letter frequencies. Although each letter in the plaintext was replaced with a different letter, the overall frequency distribution of the ciphertext was still quite similar to that of the plaintext. This is because the cipher substitutes each letter in the plaintext with a unique letter from the alphabet, maintaining the same frequency pattern, but changing the identity of each letter. Therefore, the frequency of letters was still apparent, but the letter positions and their specific identities were scrambled.



Vigenere plaintext analysis:
Once again, the plaintext followed the typical frequency distribution where letters such as 'e,' 't,' ‘I,’ and 'a' occurred more frequently than others.



Vigenere ciphertext analysis:
The Vigenère Cipher had a notable impact on the frequency distribution. By using a keyword to shift the letters in the plaintext, the ciphertext exhibited a more uniform frequency distribution. This was due to the polyalphabetic nature of the cipher, which used different shifts for each letter based on the key. As a result, the ciphertext’s letter frequencies were much less predictable, and the pattern of the original plaintext was obscured. The Vigenère Cipher provided stronger encryption by making frequency analysis much more difficult compared to the Caesar and Mono-alphabetic Substitution Ciphers.



So, can you infer character in the plaintext based only on the ciphertext?

The answer is yes. It is possible to infer characters in the plaintext based on the ciphertext for all three ciphers, but the method varies for each one.

1. **Caesar Cipher**: The Caesar Cipher is straightforward in this regard. Given the ciphertext, one can brute-force the possible shifts (ranging from 0 to 25) until a meaningful plaintext emerges. Since there are only 26 possible shifts, this process is quick and effective, making it easy to infer the plaintext once the correct shift is found.

2. **Monoalphabetic Substitution Cipher**: In the case of the Monoalphabetic Substitution Cipher, brute-forcing is impractical due to the sheer number of possible key combinations (26 factorial possibilities). However, since the cipher is a simple substitution cipher with a one-to-one correspondence between letters, language patterns still apply. The ciphertext will exhibit frequency distributions similar to those found in natural language, allowing us to make educated guesses about letter mappings. By performing frequency analysis and matching the most common ciphertext characters with those commonly used in the language (e.g., 'e', 't', 'a'), it's possible to infer the original plaintext characters. With enough ciphertext, and after recognizing the substitution patterns, the plaintext can eventually be deciphered.

3. **Vigenère Cipher**: The Vigenère Cipher complicates matters because it removes the one-to-one relationship between plaintext and ciphertext letters by using a repeating key. This means the same letter in the plaintext can be encrypted to different letters in the ciphertext, depending on the key. However, if the key length is known, the ciphertext can be divided into groups, with each group being encrypted using the same

shift. This allows for a frequency analysis on each group independently, which can be used to infer the key. The repeating nature of the key is key to breaking the cipher, as it enables a form of periodicity that can be exploited.

So, what about the Key. Can you infer the key if you know both the plaintext and the ciphertext?

Yes, the key can be inferred for all three ciphers if both the plaintext and ciphertext are known, but the process differs for each one.

1. **Caesar Cipher**: Inferring the key for the Caesar Cipher is simple. The key is simply the number of positions the letters in the plaintext are shifted to obtain the ciphertext. By comparing corresponding letters in the plaintext and ciphertext, we can determine the shift. For instance, if the letter 'A' in the plaintext is encrypted to 'D' in the ciphertext, we know the shift is 3, making the key '3'.

2. **Monoalphabetic Substitution Cipher**: The Monoalphabetic Substitution Cipher also involves mapping each plaintext letter to a corresponding ciphertext letter. Since the cipher uses a one-to-one substitution for each letter, the key can be determined by matching the ciphertext letters back to the plaintext alphabet. For longer plaintexts, this mapping becomes more apparent, and after identifying the correlations, the entire substitution key can be reconstructed.

3. **Vigenère Cipher**: The Vigenère Cipher involves a key that repeats and is applied to the plaintext letters in a cyclical manner. To infer the key, one can use the formula **(c - p) mod 26**, where **c** is the ciphertext letter, **p** is the corresponding plaintext letter, and the result is the key letter. For example, if the plaintext is "CAR" and the ciphertext is "TGF", we can calculate the key for each letter as follows:

    - For 'C' (position 2) and 'T' (position 19): (19 - 2) % 26 = 17, which corresponds to the letter 'R' in the key.

- For 'A' (position 0) and 'G' (position 6): (6 - 0) % 26 = 6, which corresponds to the letter 'G' in the key.

- For 'R' (position 17) and 'F' (position 5): (5 - 17) % 26 = 14, which corresponds to the letter 'O' in the key.

Repeating this process for each letter will reveal the full key, in this case, "RGO". With this method, we can infer the key used to encrypt the ciphertext.