1. **<u>Team name, Members</u>**
   CASE 3: Vigenere Cipher Decryption
   TEAM JIM
   - Jimmy Lam

2. **<u>Project Information and Details</u>**

- **What problems are you solving in this project?**

I am developing a program that encrypts and decrypts a plaintext/ciphertext using unique keywords that are inputted by the user running the program.

The first problem was developing a key that matched the white spaces and length of the plaintext/ciphertext.

Another problem is implementing the Vigenere cipher algorithm and how to individually encrypt/decrypt each phrase's character with each key character

- **What solutions are you implementing in this project?**

To develop this program, nested if statements and for loops will be majorly used to solve each step before incorporating the data into the Vigenere algorithm.

To solve the issue of developing a key that matches the length and white spaces of the text, I can use a for loop and if statements. By implementing logic within the if statements, I can factor out characters and whitespaces in the plaintext/ciphertext in order to add more characters to the key or add a white space to the key. Then by using a variable string, I can add all the characters and white spaces to create a new key that matches the length and white spaces of the user-inputted text.

I will be using arrays for my strings to individually encrypt/decrypt each character in the plaintext/ciphertext with each character in the key.

- **Provide an explanation of calculations and algorithm implementation.**

To develop the encryption, I am using the algorithm given in the case project document, E = (P[i] + Kl[i]) mod 26 + 65. To develop the decryption part of the program I will also be using the algorithm given in the document, D = (C[i] - K[i]) mod 26 + 65.

To solve the problem where the key length must match the length of the user-inputted text, I am using if statements and for loops. A nested if statement will be within a for loop where it repeats as long as it meets the condition that the for loop integer does not equal the value of the size of the text. The if statement logic will check if the key length does not match the length of the text and if the text has no spaces (explained later). The if statement will continue on to another if statement where it checks if the key index is null or not. If it isn't null, it will continue

and add the key index character to a string summation variable named keyTotal. However, if the key index is null, it will continue onto the else statement where the key index named keyCount (key[keyCount]) will be reset to zero and will continue on to add its index character to keyTotal. Each time the if statements are activated, the keyCount increases by one.

To solve the issue with white spaces, I have an else if statement that will activate if the text has a space character AND the key length does not match the length of the text. Once activated, it will add a space character to the summation string variable keyTotal.

When the for loop integer reaches its max value that is one less than the length of the text, it will stop and continue to the next part of the program.

The algorithm is implemented after the new key creation. Within the algorithm, it uses the user-inputted text as an array and the keyTotal array. Using a for loop where the conditions require that the index of the text is not null, it will continue onto an if statement where it checks if the current index is a space character or not. If it is a space character, a space character will be added to the string summation variable named encrypted_txt (or decrypted_txt). If there isn't a space character, it will continue onto the Vigenere algorithm part of the program where each calculation is saved onto the summation variable.

- **What are the program objectives? Explain how your program is interacting with the user and its purpose.**

The objective of the program is to take a phrase and a key from the user and to either encrypt/decrypt it using the Vigenere cipher algorithm.

For example, if the user chose to encrypt a text, if the user's input for the text was "OUTPUT" and the key was "TEST", the program will mimic the Vigenere cipher through an algorithm. It will individually match each character in the input string to each character in the key string like it would be done with a physical Vigenere cipher table. After the calculations, it will output an encrypted text.

- **How is discrete structures implemented in the C++ program?**

Discrete structures is implemented through the use of the Vigenere cipher algorithm.

E = (P[i] + Kl[i]) mod 26 + 65 is the encryption Vigenere formula where it encrypts plaintext using a key.

D = (C[i] - K[i]) mod 26 + 65 is the decryption Vigenere formula where it decrypts ciphertext using a key.

- **What are the limitations of the program?**

Efficiency is lacking as there is lots of logic while building a new key. Could be using more memory than it needs to.

- **Provide recommendations on improving the limitations of the program.**

There is definitely a better and more simplistic way that can develop a key that matches the length of the input text. Instead of slowly building the key there is surely a way that can immediately generate a new key with less logic or immediately match the user-inputted key to the plaintext/ciphertext.

3. Flowchart