CIS 7 Final Project Write-Up

CIS 7-23821

Joseph Caraan, Paul Ingram

06/03/2023

Project Information and Details

What problems are you solving in this project?

Our group decided to do Case 3, Vigenere Cypher Decryption. The problem asks us to develop a C++ program which encrypts and decrypts a message using a Vigenere table.

What solutions are you implementing in the project?

We will be using the formula where 0 <= i <= sizeof(P)
E_i = Each encrypted letter’s numerical value
P_i = Each plain text letter’s numerical value
K_i = Each key letter’s numerical value
Then, E_i = (P_i + K_i) % 26

For each decrypted letter D_i the formula will be
D_i = (E_i - K_i + 26) % 26

Provide explanation of calculations and algorithm implementation.

The calculations were given in the problem statement however we still must convert each ASCII value into its lexicographic value where A = 1, B = 2, C = 3, and so on. We will do this by looping through each letter in the plain text and subtracting a constant of 65 which is the ASCII value for ‘A’. Then we will apply the mod arithmetic formula given. Finally, we add the ‘A’ integer value back into what we got from the formula to change it back to a character and add it to the encrypted text string.

The process is identical for decrypting the encrypted text except we apply a different formula.

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

The program’s objectives are to provide the user with a choice between encrypting and decrypting text with a key. The program prompts the user to choose between encrypting or decrypting and then asks for 2 strings with one always being the key. Its purpose is to test different pairs of key and plaintext strings and see if the decryption algorithm works.

The way this program is intended to be used is to first encrypt a plain text string with a key, take the encrypted text and decrypt it with the key, then finally verify that the decrypted text matches the plain text.

How are discrete structures implemented in the C++ program?

The program uses functions that each apply an algorithm on a string to receive some kind of output. The program calls the algorithm and passes in the string pair then outputs the function. It can be modeled mathematically as f(x, y) where f is the output string for the encryption or decryption function and x, y are the plaintext/decryption string and key.

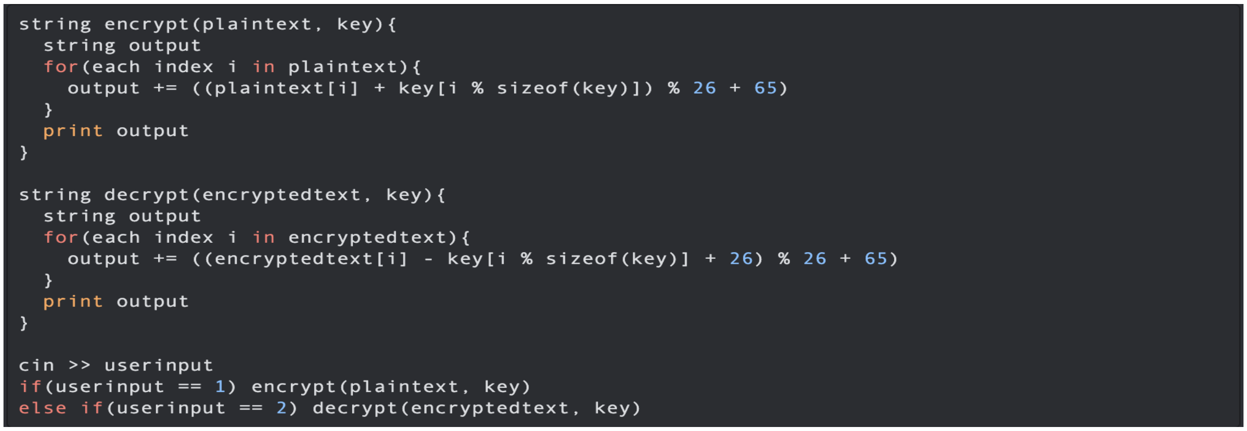
What are the limitations of the program?

The input size is limited to how big C++ stores their strings. Additionally, you can only encrypt the letters [A, Z] and no special characters. The encryption is also a simple formula that could be reversed to recover the plain text. Overall, a cipher can be the maximum length that C++ will allow but it is very simple and can be easily broken.

Provide recommendations on improving the limitations of the program.

Using mod arithmetic is probably the most efficient way to run this algorithm. The bounds are O(n) since the maximum number of times one execution of the program has to iterate is the size of the plaintext string. So, based on the limitations of C++, there is no way to improve this program.

Pseudocode



```
string encrypt(plaintext, key){
  string output
  for(each index i in plaintext){
    output += ((plaintext[i] + key[i % sizeof(key)]) % 26 + 65)
  }
  print output
}

string decrypt(encryptedtext, key){
  string output
  for(each index i in encryptedtext){
    output += ((encryptedtext[i] - key[i % sizeof(key)] + 26) % 26 + 65)
  }
  print output
}

cin >> userinput
if(userinput == 1) encrypt(plaintext, key)
else if(userinput == 2) decrypt(encryptedtext, key)
```