INTRODUCTION TO CRYPTOGRAPHY – LAB 2

B.Tech. Computer Science and Engineering (Cybersecurity)

Name: Anish Sudhan Nair	Roll No.: K041
Batch: K2/A2	Date of performance: 05/01/2022

Aim: To study about and implement the Vigenere cipher

Code:

Language: C

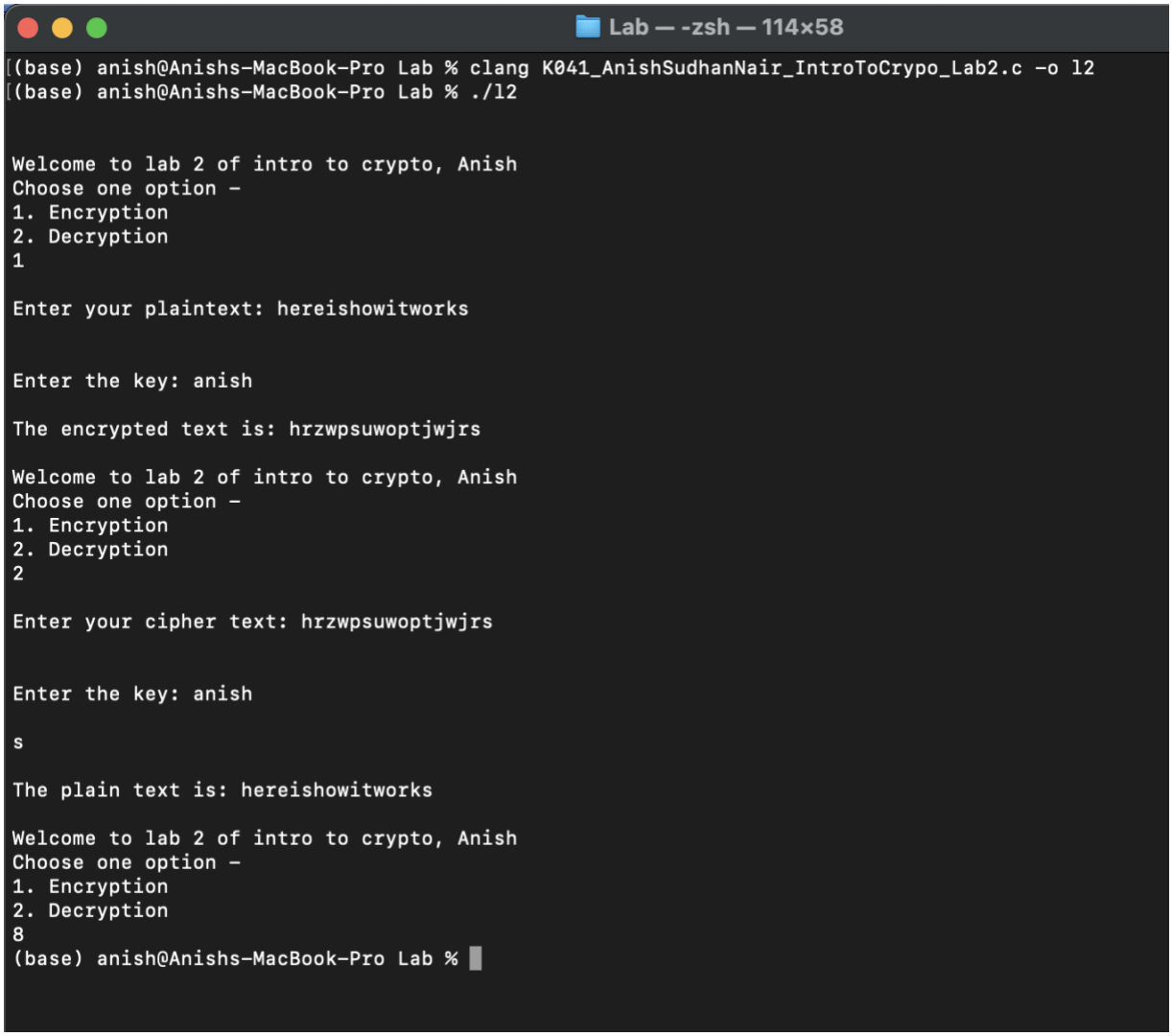
Compiler: clang/ZSH

Editor: Atom

```c
//Vigenere Cipher
#include <stdio.h>
#include <ctype.h>
#include <string.h>


int findIndex(char n){
  char alphabet[27] ={'a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z'};
  for (int i = 0; i < 26; i++) {
    if(n==alphabet[i])
      return i;
  }
  return 0;
}

void encrypt(char pln_txt[100], char key[10], char alphabet[27])
{
  int key_len=strlen(key)-1; //removing the additional line feed character
    int temp;
    int ab=5;
    char new_txt[100]="";
    char ch, temp2;

    for (int i=0, j=0;pln_txt[i]!='\n';i++,j++)
    {
      if(j==key_len)
          j=0;
      ch = tolower(pln_txt[i]);
      int posn = findIndex(ch);
      int key_posn = findIndex(key[j]);
      temp = (posn + key_posn)%26;
      if (pln_txt[i]==' ')
        {
          new_txt[i]= ' ';
          continue;
        }
      temp+='a';
      new_txt[i]= temp;
    }
    fflush(stdin);
    printf("The encrypted text is: ");
    printf("%s", new_txt);
}

void decrypt(char enc_txt[100], char key[10], char alphabet[27])
{
    int key_len=strlen(key)-1; //removing the additional line feed character
    int temp;
    char new_txt[100]="";
    char ch, temp2;

    for (int i=0,j=0;enc_txt[i]!='\n';i++,j++)
    {
        if(j==key_len)
          j=0;
        ch = tolower(enc_txt[i]);
        int posn = findIndex(ch);
        int key_posn = findIndex(key[j]);
        temp = (posn - key_posn)%26;
        if (temp<0)
```

```
            temp= (26 - key_posn + posn);
        if (enc_txt[i]==' ')
        {
            new_txt[i]= ' ';
            continue;
        }
        temp+='a';
        new_txt[i]= temp;
    }
    printf("%c\n", temp);
    printf("\nThe plain text is: ");
    printf("%s", new_txt);
}

int main()
{
    char alphabet[27] ={'a','b','c','d','e','f','g','h','i','j','k','l','m','n','o','p','q','r','s','t','u','v','w','x','y','z'};
    int n;
    char key[100];
    char pln_txt[100], enc_txt[100];

    do{
        printf("\n\nWelcome to lab 2 of intro to crypto, Anish");
        printf("\nChoose one option - \n1. Encryption \n2. Decryption\n");
        scanf("%d", &n);
        while ((getchar()) != '\n');

        switch(n)
        {

            case 1:
            fflush(stdin);
            printf("\nEnter your plaintext: ");
            fgets(pln_txt, sizeof(pln_txt), stdin);
            while ((getchar()) != '\n');
            printf("\nEnter the key: ");
            fgets(key, sizeof(key), stdin);
            while ((getchar()) != '\n');
            encrypt(pln_txt, key, alphabet);
            break;

            case 2:
            printf("\nEnter your cipher text: ");
            fgets(enc_txt, sizeof(enc_txt), stdin);
            while ((getchar()) != '\n');
            printf("\nEnter the key: ");
            fgets(key, sizeof(key), stdin);
            while ((getchar()) != '\n');
            decrypt(enc_txt, key, alphabet);
            break;

            default:
            n=4;
        }
    }while(n!=4);

    return 0;
}
```

Output:



Questions:

1. Explain the working of Vigenere Cipher

   Vigenere Cipher is a polyalphabetic cryptosystem that uses an alphabetic keyword of a particular length to encrypt the plain text. We first convert the letters to the assigned numbers (A=0, B=1, C=2…etc) and then add the numeric values of the plain text and the keyword, and upon exhausting the keyword we start from the first letter of the keyword again; this continues until the entire plain text has been exhausted. We finally convert the numbers to their respective letters.

   For decryption we do the exact reverse of the encryption process by subtracting the numeric value of the keyword from the cipher text and then converting it back to the alphabet.

2. List the advantages and limitations of Vigenere Cipher

   Vigenere Cipher is a great improvement over the Caesar Cipher and is not susceptible to frequency analysis since due to the repeating nature of the keyword, each letter doesn't necessarily correspond to one particular letter post encryption.

   The repeating nature of the keyword is also the cipher's greatest disadvantage. If a person is able to even merely guess the length of the keyword correctly they could use the Kasiski method or the Friedman test to decrypt it.

3. Compare and contrast mono alphabetic and poly alphabetic ciphers

   Monoalphabetic ciphers as the name suggests rest on the bedrock that the letters or symbols in a plain text and the corresponding cipher text enjoy a one-to-one relationship wherein every symbol has a fixed symbol it relates to. It is a simple single substitution cipher and is therefore easier to crack.

   Polyalphabetic ciphers on the other hand enjoy a one-to-many relationship between the plain text and its corresponding cipher text where a single element may be encrypted as more than one symbol. It is a multiple substitution cipher often a layer of complexity over the simpler monoalphabetic ones, such as a Vigenere cipher essentially being interwoven Caesar ciphers and is therefore tougher to crack.