**HỌ TÊN: TRỊNH XUÂN CHINH – TH24.09**

**BÀI TẬP VÀ THỰC HÀNH HỌC PHẦN BẢO MẬT: (*BUỔI 3*)**

**Bài tập 1:** Cho biến đọan mã sau dùng mã Ceasar

"CSYEVIXIVQMREXIH"

Suy luận tìm bản rõ (sử dụng bảng chữ cái tiếng Anh).

YOU ARE TERMINATED

**Bài tập 2:** Sử dụng kỹ thuật thám mã bảng chữ đơn, lập bảng tần suất các chữ, bộ chữ đôi, bộ chữ ba của đọan mã sau:

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIVUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSXEPYEPOPDZSZUFPOUDTMOHMQ

Lập luận và cho biết ánh xạ của bảng chữ đơn và đưa ra bản rõ phù hợp

**Bài tập 3:** Tìm bản mã của bản rõ “CHUNG TOI LA SINH VIEN CNTT HUBT” sử dụng mã Playfair với từ khóa “KINH DOANH CONG NGHE”.

GNSDM YAK FC RNHD WKCD LCSY DTMQ

**Bài tập 4:** Mã hóa bản rõ “CONG NGHE THONG TIN THE KY 21” sử dụng từ khóa 631425 bằng phương pháp Vigenere.

XWTK AKYI OPURT XZR OPK OL 21

**Bài tập 5:** Cho hệ mã Vigenere có M = 6, K = “LEG”.

1. Hãy thực hiện mã hóa xâu P = “THIS IS ROBOT SOPHIA“.

ELODTODTXZFUETYZTNTE

1. Hãy thực hiện giải mã xâu M = “PBVWEOYEZTST”.

EXPLAINATION

**Bài tập 6:** Cho hệ mã Vigenere . Biết bản mã “PVRLHFMJCRNFKKW” có bản rõ tương ứng “ Networksecurity” Hãy tìm khóa K ??

1. Hãy tìm khóa mã hóa đã dùng của hệ mã trên.

CRYPTO

1. Dùng khóa tìm được ở phần trên hãy giải mã bản mã C = “KLGZWT OMBRVW”.

IUIKDF MVDCCI

**Bài tập 7:** Cho hệ mã Vigenere có M = 6. Mã hóa xâu P = “SPIRIT“ người ta thu được bản mã là “OXHRZW”.

1. Hãy tìm khóa mã hóa đã dùng của hệ mã trên.

WIZARD

1. Dùng khóa tìm được ở phần trên hãy giải mã bản mã C = “BQETYH HMBEEW”.

FIFTHE LECENT

**Bài tập 8:** Cho hệ mã Vigenere có M = 6. Giải mã xâu C = “RANJLV” người ta thu được bản rõ là “CIPHER”.

1. Tìm khóa đã sử dụng của hệ mã trên.

PSYCHE

1. Dùng khóa tìm được ở phần trên hãy hãy giải mã xâu M = “PLDKCI DUJQJO“.

NDODYR BMUJFX

Sử dụng một trong các ngôn ngữ lập trình C, C++, Java hoặc C# để làm các bài tập sau:

**Bài tập 9**: Viết chương trình đếm tần số xuất hiện của các chữ cái tiếng Anh trong một văn bản tiếng Anh ở dạng file text.

**Bài tập 10**: Viết chương trình cài đặt thuật toán mã hóa và giải mã của hệ mã Ceasar.

#include<iostream>

#include<string.h>

using namespace std;

int main() {

   cout<<"Enter the message:\n";

   char msg[100];

   cin.getline(msg,100); //take the message as input

   int i, j, length,choice,key;

   cout << "Enter key: ";

   cin >> key; //take the key as input

   length = strlen(msg);

   cout<<"Enter your choice \n1. Encryption \n2. Decryption \n";

   cin>>choice;

   if (choice==1) //for encryption{

      char ch;

      for(int i = 0; msg[i] != '\0'; ++i) {

         ch = msg[i];

         //encrypt for lowercase letter

         If (ch >= 'a' && ch <= 'z'){

            ch = ch + key;

            if (ch > 'z') {

               ch = ch - 'z' + 'a' - 1;

            }

            msg[i] = ch;

         }

         //encrypt for uppercase letter

         else if (ch >= 'A' && ch <= 'Z'){

            ch = ch + key;

            if (ch > 'Z'){

               ch = ch - 'Z' + 'A' - 1;

            }

            msg[i] = ch;

         }

      }

      printf("Encrypted message: %s", msg);

   }

   else if (choice == 2) { //for decryption

      char ch;

      for(int i = 0; msg[i] != '\0'; ++i) {

         ch = msg[i];

         //decrypt for lowercase letter

         if(ch >= 'a' && ch <= 'z') {

            ch = ch - key;

            if(ch < 'a'){

               ch = ch + 'z' - 'a' + 1;

            }

            msg[i] = ch;

         }

         //decrypt for uppercase letter

         else if(ch >= 'A' && ch <= 'Z') {

            ch = ch - key;

            if(ch < 'A') {

               ch = ch + 'Z' - 'A' + 1;

            }

            msg[i] = ch;

         }

      }

      cout << "Decrypted message: " << msg;

   }

}