Cifratura di Vigenère

Il programma implementa l'algoritmo di Vigenere per cifrare / decifrare file di testo con più di un alfabeto cifrante.
L'algoritmo di Vigenere dice che le lettere di un testo da cifrare possono essere spostate anche di diverse posizioni (non solo una come il Cifrario di Cesare) basta che si ripetino. Le lettere spostate si possono facilmente individuare dalla seguente matrice:

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
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 A
C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
V W X Y Z A B C D E F G H I J K L **M** N O P Q R S T U
W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
Z 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

Le posizioni che spostano la lettera indicano le righe della matrice, mentre per trovare la lettera corrispondente si guarda nella riga della posizione e nella colonna della lettera da cifrare, quella che viene fuori è la lettera cifrata.
Per decifrare il testo il destinatario deve conoscere ovviamente la chiave di cifratura, per sapere in quali righe della matrice guardare. Per risalire al testo originale, deve guardare la riga della matrice indicata dalle posizioni e trovare la lettera corrispondente al testo cifrato, dopodiché risale la colonna fino ad arrivare alla prima riga della matrice (che è il nostro alfabeto di riferimento) e trova la lettera originale.
Ecco un esempio per far capire meglio:
Devo cifrare il messaggio: ciao sono Luca
Con la chiave 2 – 4 – 5 – 3
Intanto posiziono i numeri sotto alle lettere corrispondenti:

c i a o	s o n o	L u c a
2 4 5 3	2 4 5 3	2 4 5 3

La prima lettera del testo cifrato diventa una D, infatti vado nella riga 2 della matrice, la scorro finchè non vedo che sopra alla lettera corrispondente non ci sia la C.
La seconda lettera diventa una L, sempre con lo stesso procedimento di prima.
Alla fine il testo cifrato diventa:

dleq trrq mxgc

Per decifrare posiziono i numeri come ho fatto prima per cifrare e diventa:

d l e q	t r r q	m x g c
2 4 5 3	2 4 5 3	2 4 5 3

Poi vado nella seconda riga della matrice, guardo la lettera D e salgo la sua colonna fino ad arrivare alla prima riga della matrice trovando la C, che è la lettera originale. Facendolo fino alla fine il messaggio diventa:

ciao sono Luca

Che è proprio il messaggio originale.

I numeri delle posizioni usati per la chiave indicano il numero di alfabeti cifranti.

Nel programma l'utente può scegliere se cifrare o decifrare il testo, poi deve inserire il testo e la chiave. Per maggiore sicurezza il programma chiede l'inserimento di almeno 4 numeri di chiave per usare almeno 4 alfabeti cifranti. I numeri sono da inserire separati da un punto e virgola, secondo la seguente stringa:

num1;num2;num3;num4 e 4 è il numero di chiavi

I numeri devono essere compresi fra 2 e 26, in quanto la prima riga è il nostro alfabeto e non viene considerato cifrante, mentre numeri superiori a 26 non corrispondono a nessun alfabeto.
Non c'è un numero massimo di chiavi da utilizzare in teoria, anche se in pratica al massimo possono essere 2 ^ 31, in quanto nel ciclo che scorre gli elementi della chiave viene usata una variabile int che al massimo può raggiungere il valore 2 ^ 31 e di conseguenza il programma si bloccherebbe perché non riesce più ad uscire dal ciclo in quanto la condizione resterebbe sempre vera, perché in una variabile int 2 ^ 31 + 1 è uguale a - 2 ^ 31.
Bisogna anche dire che un numero di chiavi maggiore delle lettere del testo da cifrare non ha senso inserirle, perché i numeri in più non si possono incolonnare a nessuna lettera. Vigenere diceva che l'ideale era usare un numero di chiavi pari al numero di lettere del testo.
Se l'utente inserisce una chiave composta da tutti numeri uguali il programma da un messaggio di errore, in quanto sarebbe come se usasse un solo alfabeto cifrante.

Il programma usa una matrice di riferimento (come quella sopra) e altri 2 vettori di riferimento: uno che contiene tutti i valori possibili della chiave (cioè stringhe da 2 a 26 e anche la stringa vuota) e uno che contiene la prima riga della matrice (vettore di caratteri, serve per inizializzare la matrice con un ciclo da 10 righe invece che con le assegnazioni singole che sarebbero 26*26 = 676 righe di codice).

Per inserire il testo nella text box l'utente può anche trascinare un file di testo .txt dal computer alla text box (drag and drop).

Per non fare impazzire il programmatore, tutto il testo in input da cifrare viene convertito in lettere minuscole, in questo modo la matrice di riferimento è solo una, anche se il testo in output contiene solo lettere minuscole; quando viene decifrato le lettere che prima erano maiuscole diventano tutte minuscole.
Nella cifratura / decifratura i caratteri speciali non vengono considerati (per esempio lo spazio, la virgola, …) e vengono lasciati tali e quali.

Il programma salva un file ti testo.txt per mostrare l’output all’utente.