Cryptage poly-alphabétique

Travaux Pratiques 05 du module 05 - Les variables complexes

Avant de démarrer ce TP, il convient d'avoir suivi les vidéos des modules 1 à 6 de ce cours.

Durée estimée
Environ 2 heures

Énoncé

Mettre en place un programme permettant de crypter ou décrypter une chaîne saisie en fonction d'une clé saisie entre 4 et 16 caractères.

Exemples

- Chiffrage :
  - Message (en clair) : « **`On débarque demain sur la plage`** »
  - La clef : **`OMAHA`**
    - Message normalisé : `ON DEBARQUE DEMAIN SUR LA PLAGE`
    - Répétition de la clef : **`OM AHA`**`OMAHA OMAHAO MAH AO MAHAO`
    - Message chiffré : **`CZ DLBODQBE RQMHIB EUY LO BLHGS`**
- Déchiffrage (opération inverse) :
  - Message chiffré : « `RXUIYEMFR : JP J LYIE EID ESLVJWEPW !` » (Déjà normalisé)
  - Avec une mauvaise clef : *`ALLIANCE`*
    - Message déchiffré : ~~`RMJAYRKBR : YE B LLGA EXS WSYIFWTEO !`~~
  - Avec la bonne clef : **`REBELLE`**
    - Message normalisé : `RXUIYEMFR : JP J LYIE EID ESLVJWEPW !`
    - Répétition de la clef : **`REBELLE`**`RE BE L LERE BEL LEREBELLE`
    - Message en clair : **`ATTENTION : IL Y AURA DES TOURISTES !`**

Explication

Pour réaliser ces deux opérations à partir d'une phrase saisie, il faut utiliser la matrice (de la page suivante) dans laquelle est affiché autant d'alphabets qu'il y a de lettres (26) avec un décalage :

- Pour chiffrer, on cherche la lettre du message sur la colonne, et la lettre de la clef sur la ligne. L'intersection des deux permet d'obtenir une nouvelle lettre pour construire le message crypté. Puis on passe à la lettre suivante, et lorsque l'on atteint la limite des lettres de la clef, on revient au début de celle-ci et ainsi de suite.
- Inversement pour de déchiffrage, on recherche la lettre de la clef la ligne, dans cette ligne on recherche la lettre chiffrée, puis on remonter sur l'axe de la colonne afin de révéler la lettre d'origine, et ainsi de suite sur le même principe.

Concept

- À partir de la matrice ci-dessous, il est possible de déterminer par intersection les lettres pour réaliser les opérations de cryptage et inversement :

→ Axe pour le message en clair

↓ Axe de la clef de cryptage

	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

➔ L'intersection des axes colonne/ligne permet d'obtenir la lettre du chiffrement pour crypter le message ou bien le déchiffrer. Par exemple : `MESSAGE + SECRET = EIUJEZW`

Conseils

Procéder étapes par étapes, afin de fiabiliser votre mécanisme.

Utiliser des constantes pour tester toujours le même mot (déjà normalisé) avant de tester une phrase, afin d'éprouver votre mécanisme. Ne cherchez pas à optimiser dès le début.

Nommez convenablement vos variables, afin de ne pas être perdu dans leurs utilisations.

Objectif / Niveau

1. Essentiel : Générer et afficher la matrice qui sera utilisée pour le chiffrement.
2. Attendu : Mettre en place le mécanisme de cryptage par la saisie d'une clef.
3. Avancé : Procéder à l'écriture du mécanisme inverse, afin de décrypter un message.

Solution

Des propositions de solution pour ce TP sont placées dans les éléments en téléchargement liés à ce module. (https://fr.wikipedia.org/wiki/Chiffre_de_Vigen%C3%A8re)

Astuces

Vous pouvez saisir du texte déjà normaliser pour aller plus vite. Sinon, intéressez-vous à la méthode « translate() » à partir de tables pour ignorer les caractères accentués et autres.