TP Maple 6 | Codages de César et de Vigenère

Le texte suivant est librement inspiré de l'épreuve écrite d'informatique posée à l'Ecole Polytechnique en 2008 dans la filière MP (option SI)

On cherche à crypter (i.e. à coder) un message donné en Français, composé de caractères (les 26 *lettres de l'alphabet) en minuscules, non accentués et sans aucun espace entre les mots. Le message est donné sous la forme d'une liste* **L** *de lettres minuscules. Pour illustrer ce qui suit, nous utiliserons le message* **jansondesailly** *représenté par la liste* **L** *suivante de longueur* 14 *:*

Liste **L**	**j**	**a**	**n**	**s**	**o**	**n**	**d**	**e**	**s**	**a**	**i**	**l**	**l**	**y**
Indices dans **L**	1	2	3	4	5	6	7	8	9	10	11	12	13	14

Ainsi, **L[2] = a** *et* **L[11] = i**. *Effectuant plus facilement des opérations sur les nombres que sur les lettres (grâce à l'arithmétique, etc.), nous commencerons par transformer les messages en nombres.*

1. Chiffrage et déchiffrage d'un message

La lettre **a** *est remplacée par* 1, **b** *par* 2, *et ainsi de suite jusqu'à* **z** *remplacée par le nombre* 26. *Un message* **L** *sera donc transformé en une liste de nombres* **C** *:*

Liste **L**	**j**	**a**	**n**	**s**	**o**	**n**	**d**	**e**	**s**	**a**	**i**	**l**	**l**	**y**
Liste **C**	**9**	**0**	**12**	**18**	**14**	**12**	**3**	**4**	**18**	**0**	**8**	**11**	**11**	**24**
Indices dans **L** et **C**	1	2	3	4	5	6	7	8	9	10	11	12	13	14

Cette opération s'appelle le chiffrage. En utilisant la correspondance réciproque (remplacer un nombre entre 1 *et* 26 *par la lettre correspondance), on peut effectuer l'opération inverse : transformer une liste de nombres* **C** *en un message* **L**. *C'est l'opération de déchiffrage.*

1. Définir une table **LC** et une liste **CL**, indexées respectivement par les lettres **a, b, . . . , z** et les nombres $1, 2, \ldots, 26$, telles que

$$\begin{cases} \mathbf{LC[a] = 1,\ LC[b] = 2,\ \ldots,\ LC[z] = 26} \\ \mathbf{CL[1] = a,\ CL[2] = b,\ \ldots,\ CL[26] = z} \end{cases}$$

2. Ecrire une procédure **Chiffrage(L)** retournant le chiffrage **C** d'un message **L** donné.

3. Ecrire une procédure **Dechiffrage(C)** retournant le déchiffrage **L** d'une liste de nombres **C** donnée.

2. Le codage de César

Le codage de César est le plus rudimentaire que l'on puisse imaginer. Il a été utilisé par Jules César (et même auparavant...) pour certaines de ses correspondances. Le principe est de décaler les lettres de l'alphabet vers la droite de une ou plusieurs positions. Par exemple, en décalant les lettres d'une position, le caractère **a** *se transforme en* **b**, *le* **b** *en* **c**, ..., *et le* **z** *en* **a**. *Le message* **jansondesailly** *est donc codé par* **kbotpoeftbjmmz**.

2.1. Codage et décodage d'un texte connaissant la clé

1. Que donne le codage de **myrtille** pour un décalage de 5 lettres ?

2. Ecrire une procédure **CodageCesar(L,d)** prenant en argument un message **L** et un décalage **d**, et qui retourne le message **L** décalé de **d** lettres.

3. Ecrire une procédure **DecodageCesarAvecCle(L,d)** prenant les mêmes arguments et mais qui réalise le décodage d'un message codé **L**.

2.2. Casser » un code de César

Pour réaliser ce décodage, il faut connaître la valeur du décalage **d**, *appelée* clé *du codage. Une manière de la déterminer automatiquement est d'essayer de deviner cette valeur. L'approche la plus couramment employée est de regarder la fréquence d'apparition de chaque lettre de l'alphabet dans le message crypté. En effet, la lettre la plus fréquente dans un texte suffisamment long en français est le* **e**.

1. Ecrire une procédure **Frequences(C)** qui prend en argument une liste **C** représentant le chiffrage du message codé et qui retourne la liste de taille 26 dont la case d'indice $1 \leqslant i \leqslant 26$ contient le nombre d'apparitions du nombre i dans la liste chiffrée **C**.

2. Ecrire une procédure **Cle(C)** qui prend en argument une liste **C** représentant le chiffrage du message codé et qui retourne la valeur de la clé, i.e. la valeur du décalage **d** utilisé.

3. Ecrire une procédure **DecodageCesar(L)** qui prend en argument un message codé **L** et qui retourne le *message d'origine*.

2.3. Exemples

1. Trouver le codage du texte (immortel...) suivant pour un décalage de 11 :

jepreferelatarteauxmyrtillesalapfelstrudel

2. Décoder le texte suivant :

hlvarzdvmfzityvivzeufcvekvuvkfetfigjjzsvrltfddvlevvkfwwvmrtzccrekvdzifzkvicrgvrl

3. Le codage de Vigenère

Au XVI^e *siècle, Blaise de Vigenère a modernisé le codage de César très peu résistant de la manière suivante. Au lieu de décaler toutes les lettres du texte de la même manière, on utilise un texte clé qui*

donne une suite de décalages. Prenons par exemple la clé **concours**. *Pour coder un texte, on code la première lettre en utilisant le décalage qui envoie le* **a** *sur le* **c** *(la première lettre de la clé). Pour la deuxième lettre, on prend le décalage qui envoie le* **a** *sur le* **o** *(la seconde lettre de la clé) et ainsi de suite. Pour la huitième lettre, on utilise le décalage de* **a** *sur* **s**, *puis, pour la neuvième, on reprend la clé à partir de la première lettre.*

1. Donner le codage du texte **becunfromage** en utilisant la clé **jean**.

2. Ecrire une procédure **CodageVigenere(L,Cle)** prenant comme arguments le message **L** à coder et la clé choisie sous la forme d'une liste **Cle**.

3. Ecrire une procédure **DecodageVigenere(L,Cle)** prenant comme arguments le message **L** à décoder et la clé sous la forme d'une liste **Cle**.

« Casser » un code de Vigenère s'avère plus délicat que décrypter un code de César. Le lecteur curieux consultera à ce sujet l'épreuve écrite d'informatique posée au concours d'admission 2008 de l'Ecole Polytechnique dans la filière MP (option SI).