Cryptage de chaînes de caractères

Ce TD propose de programmer différentes méthodes pour crypter ou décrypter des messages.

1. Jules César, le célèbre empereur romain, rendait illisibles ses messages au cas où ils tomberaient entre les mains de ses ennemis. Sa technique était simple : il utilisait le chiffrement par décalage.

   Imaginons que Jules César souhaite envoyer le message suivant à un de ses généraux :

   « Ce soir, on attaque les Gaulois ! »

   Jules César, qui aimait utiliser le chiffre 3 comme clé de chiffrement, procéde alors comme suit :

   Le message commence par « C », c'est la troisième lettre de l'alphabet. $3 + 3 = 6$, « F »est la sixième lettre de l'alphabet. « C »est donc remplacé par « F ».

   La deuxième lettre est « E », c'est la cinquième lettre de l'alphabet. $5 + 3 = 8$. « H »est la huitième lettre de l'alphabet. « E »est donc remplacé par « H ».

   Finalement, le message crypté donne :

   « FH VRLU, RQ DWWDTXH OHV JDXORLV ! »

   Par la suite, le général, une fois le message reçu, procède à l'inverse pour le déchiffrer. « F »est la sixième lettre de l'alphabet. $6 - 3 = 3$. « F »remplace donc « C ». « H »est la huitième lettre de l'alphabet. $8 - 3 = 5$. « H »remplace donc « E ».

   NB : Avec cette méthode, X est remplacé par A, Y par B et Z par C si l'on décale de 3.

   (a) Écrire une fonction, $decale(caractere, nb)$, qui étant donné un caractère en majuscule, renvoie le caractère obtenu en décalant de l'entier nb selon la méthode de chiffrement de César.

   On prendra soin de ne pas modifier les caractères qui ne sont pas des lettres en majuscules et de les renvoyer tels quels.

   Indication : on poura utiliser les fonctions suivantes :
   — $ord(caractere)$ qui renvoie le numéro d'un caractère $caractere$ donné. $ord('A')$ renvoie 65 par exemple, $ord('B')$ donne 66,$\cdots$, $ord('Z')$ renvoie 90.
   — $chr(nombre)$ renvoie le caractère de numéro $nombre$. $chr(65)$ renvoie $'A'$ par exemple.

   (b) Écrire alors une fonction $chiffre(message, nb)$ qui prend en argument une chaîne de caractères $message$ et qui renvoie cette même chaînes dont tous les caractères en majuscules ont été décalés du nombre nb selon la méthode de César.

   (c) Écrire enfin une fonction $dechiffre(message, nb)$ qui permette de l'inverser, de préférence à l'aide de la fonction précédente.

2. Les Grecs utilisaient une scytale pour coder leurs messages. La technique était aussi simple qu'astucieuse. L'expéditeur enroulait une lanière de cuir autour d'un bâton et écrivait son message dans le sens de la longueur. Une fois la lanière déroulée, le message devenait illisible puisque les lettres se retrouvaient alors dans le désordre.

   Concrètement, avec une clé de 5 et le message « Nous nous battrons jusqu'au bout », cela donne la matrice à 5 colonnes suivantes :

$$\begin{pmatrix} N & o & u & s & \\ n & o & u & s & \\ b & a & t & t & r \\ o & n & s & & j \\ u & s & q & u & ' \\ a & u & & b & o \\ u & t & & & \end{pmatrix}$$

   Et l'on transmet le message « Nnbouauooansutuutsq sst ub rj'o »en écrivant les caractères des différentes colonnes de la matrice dans l'ordre.

   Ce chiffrement consite en quelque sorte à mettre les caractères dans une matrice dans l'ordre des lignes succesives, la transposer et lire le message à transmettre sur les lignes de la matrice ainsi obtenue. NB : s'il reste de la place dans la matrice, on la complète avec des espaces lorsque le nombre de caractères du message n'est pas divisible par la clé.

   (a) Ecrire une fonction, $crypte(chaine, cle)$ qui applique cette méthode pour crypter le message *chaine*, qui prend la forme d'une chaîne de caractères, à l'aide d'une matrice à *cle* colonnes et renvoie le message crypté.

   (b) Ecrire enfin la fonction de décryptage. Il est recommandé encore une fois de réutiliser la fonction de cryptage.