

CI 8: Chaînes de caractères

Télécom Physique Strasbourg — October 3, 2021

Exercices complémentaires

Exercice C14 (*Cryptographie par rot13*)

Parmi les méthodes de chiffrement existantes, les plus simples utilisent un principe de clef symétrique ou clef secrète pour chiffrer et déchiffrer l'information. Le code de César est la méthode de cryptologie la plus ancienne communément admise par l'histoire. Ce code consiste à remplacer chaque lettre du texte par celle qui se trouve N places plus loin dans l'alphabet, N étant la clef. Par exemple, pour chiffrer une chaîne de caractères avec cette technique, en utilisant une clef de 3 : TPS devient GCF et Colin devient Frolq. Le principal problème d'une telle méthode est que la clé doit être transmise au destinataire, avec le risque qu'elle soit interceptée. Une autre limitation est qu'une analyse statistique du texte chiffré permet de retrouver la clef, et donc le texte de départ, si ce texte n'est pas trop court.

Cette méthode a été reprise sur les forums de discussion sous le nom de rot13, qui utilise un décalage de 13 lettres de l'alphabet. Il est ainsi utilisé non pas pour rendre secret un message (facile à décoder) mais pour éviter que ne soit lu par inadvertance un propos choquant ou de "spoiler" la fin d'un film/roman. L'intérêt du rot13 est que le chiffrement et déchiffrement se fait exactement par le même algorithme, car il y a 26 lettres dans l'alphabet et le décalage est circulaire (arrivé à 'z', on continue avec 'a').

Écrire un programme qui réalise un chiffrement rot13 d'un texte non accentué (la ponctuation reste telle quelle). Tester votre fonction en codant et décodant un même message.

On pourra comparer ou décoder la sortie de son programme avec le rot13 disponible en ligne sur <http://rot13.com>.



Exercice C15 (*Conversion*)

Écrire un programme qui lit une phrase de la forme 14 pouces ? Ou 3 cm ? et donne la correspondance dans l'autre unité.

Exemple :

14 pouces ? ↔
90.47 cm
13 cm ? ↔
5.12 pouces

Note: 1cm = 0,394 pouces et 1 pouce = 2,54cm