IREM de Clermont-Ferrand
Formation ISN
Algorithmique et programmation

7 novembre 2013
Malika More
malika.more@u-clermont1.fr

Cryptographie

Chiffrement par décalage

- Un chiffrement par décalage consiste à décaler les lettres de l'alphabet d'une valeur fixe.
- Et bien sûr, si on dépasse Z, on reprend à partir de A.

Exercice 1 (Chiffre de César)**.** Les lettres de l'alphabet sont chiffrées à l'aide d'un décalage de 4 lettres vers la droite. Cette méthode est réputée avoir été utilisée par Jules César pour communiquer secrètement avec ses généraux pendant la guerre des Gaules, d'où son nom.

1. Chiffrer le message : ALLEZ-Y.
2. Quelle est la clé de déchiffrement du chiffre de César ?
3. Déchiffrer la réponse du général : SR C ZE

Exercice 2 (Une faiblesse dangereuse)**.** Combien y-a-t-il de chiffrements par décalage différents ?

Exercice 3 (Une faille de sécurité)**.** Le cryptogramme suivant a été obtenu à l'aide d'un chiffrement par décalage inconnu : TZTVIFE VJK LE REV. Un espion habile a réussi à découvrir que la lettre S est chiffrée par la lettre J.

1. Décrypter le message proposé.
2. Préciser quelles sont les clés de chiffrement et de déchiffrement correspondantes.

Exercice 4 (Décryptage)**.** Le cryptogramme suivant a été obtenu à l'aide d'un chiffrement par décalage inconnu :

TOX VXLTK !
C'TB VTIMNKX NG XLIBHG.
T UBXGMHM,
LBZGX : FTKV-TGMHBGX

1. Proposer deux méthodes de décryptage (impliquant éventuellement l'utilisation d'un ordinateur), l'une tirant parti de l'exercice 2, et l'autre de l'exercice 3.
2. Décrypter le message proposé.
3. Préciser quelles sont les clés de chiffrement et de déchiffrement correspondantes.

Exercice 5 (Programmation)**.** Écrire des fonctions de chiffrement, déchiffrement et décryptage d'un code par décalage. Les textes seront entrés au clavier en majuscule et sans accents. On conservera les espaces et la ponctuation.