INF808 – LAB1

Question 1 :

*Au vu du code du listing 1 expliquer comment la représentation numérique d’un caractère permet d’implémenter une translation de caractère ?*

Un caractère est encodé sur un octet de 8 bits. Un charactère est d’abord un nombre binaire, qui peut être ensuite translaté en nombre décimale/hexadécimale. La table ASCII est un standard de représentation des charactères. Les caractères alphabétiques de [a-z] sont définit à partir du nombre 97 en décimale, 67 en hexadécimale jusqu’à 122 en décimale, 7A en hexadécimale. Grâce à ce standard, la représentation des caractères est universelle.

Question 4 :

*Expliquer et trouver deux clés différentes k et k 0 qui donnent un même chiffré. En déduire le nombre (minimal) de clés qui, pour un texte claire donné, fournissent des chiffrés différents*

Prenons k = 1, k’ = 27. Si on utilise la fonction encrypt(‘abc’,k) et encrypt(‘abc’,k’). On retombe sur le même chiffré. Cela s’explique car il y a 26 caractères différents dans l’alphabet et donc le chiffrement est lié à ce modulo 26. On en déduit donc qu’il y a 25 clés différentes car k > 0.

*Expliquer pourquoi le code de Cæsar se prête à une attaque de force brute et décrire comment vous procèderiez à une attaque de type brute force pour décoder un chiffré dont vous n’avez pas la clé k.*

Avec un peu d’analyse, on déduit que l’attaque par force brute prendra un temps en complexité O(n). Pour procéder à une attaque de force brute, vu qu’il n’y a que 25 permutations possibles on va chercher parmi les 25 possibilités après décalage de +1 à chaque tour de boucle le message qui nous parait le plus probable à être déchiffré.