Mathématiques à l'Usage des Informaticiens

Erkin Tunç Boya

Décembre 2023

Table des matières

1 Méthodes de Cryptologie

1.1 Code Inverse

Il s'agit de crypter un message en inversant son écriture. Le décrypter revient au même. Un seul programme sera utilisé en considérant qu'on est en mode cryptage ou décryptage.

1.1.1 Les fonctions

— `crypter(message)`
— `decrypter_crypt(message)`

1.2 Code César Simple

Pour crypter, on décale chaque lettre de b indices où b est la clé de chiffrement. Crypter le message x avec la clé b sur un alphabet de taille n : $y \equiv x + b \mod n$, où y est le message obtenu.

Décrypter le message x avec la clé b sur un alphabet de taille n : $y \equiv x - b \mod n$, où y est le message obtenu.

La clé b est un nombre entier et une variable indique en quel mode agit (cryptage ou décryptage).

1.2.1 Les fonctions

— `decalage_mot(mot, k)`
— `decryptage_decalage_mot(mot, k)`

1.3 Code de Vigenère

Ce code permet de crypter le message. Le décalage change de lettre en lettre grâce à une clé. Pour chiffrer un message, on décale chaque lettre du message par le même décalage qui fait passer la lettre "a" à la lettre correspondante de la clé écrite sous le message (et répétée autant de fois que nécessaire).

1. L'alphabet peut changer (mais si tu changes, n'oublie pas de modifier de fonctions (Cryptage/Décryptage Vigenere)).
2. Si une lettre du message n'est pas dans l'alphabet, le code la laisse inchangée.

1.3.1 Les fonctions

— `creationDic(liste_biblio)`
— `liste_decalage(message, cle, bibliotheque)`
— `Cryptage_Vigenere(message, cle)`
— `Decryptage_Vigenere(message_crypte, cle)`

Les fonctions utilisent comme ci-dessous :
— `Cryptage_Vigenere(message, cle)`
  — `creationDic(li_biblio)`
  — `liste_decalage(message, cle, bibliotheque)`
— `Decryptage_Vigenere(message_crypte, cle)`
  — `creationDic(li_biblio)`
  — `liste_decalage(message, cle, bibliotheque)`

1.4 Code César Affine

Crypter le message x avec les clés a et b sur un alphabet de taille n : $y \equiv ax+b \mod n$, où y est le message obtenu.

Décrypter le message x avec les clés a' et b' : $y \equiv a'x + b' \mod n$, où y est le message obtenu.

1. Les clés a et b sont des nombres entiers.
2. Les fonctions rendent toutes les lettres en minuscules parce que l'alphabet contient seulement des lettres minuscules (Modifie et agrandit l'alphabet pour le majuscule).

1.4.1 Les fonctions

— `pgcd(a, b)`
— `creationDic(liste_biblio)`
— `Cryptage_CesarAffine(message, cle_a, cle_b)`
— `Decryptage_CesarAffine(message_crypte, cle_a, cle_b)`

Les fonctions utilisent comme ci-dessous :
— `Cryptage_CesarAffine(message, cle_a, cle_b)`
  — `pgcd(a, b)`
  — `creationDic(liste_biblio)`
— `Decryptage_CesarAffine(message_crypte, cle_a, cle_b)`
  — `pgcd(a, b)`
  — `creationDic(liste_biblio)`

2 Jeux D'essais

2.1 Exemple 1

Le message est "Si deux hommes ont la même opinion. L'un d'eux est de trop."
K = 3
CLE = "hope"

2.2 Exemple 2

Le message est "Chez moi, le secret est enfermé dans une maison aux solides cadenas dont la clé est perdue et la porte scellée." - Les mille et une nuits
K = 2
CLE = "2023"

2.3 Exemple 3

Le message est "'snoçel sed ennod em no uq sruojuot sap emia n ej euq neib erdnerppa a terp sruojuot sius ej'"
K = 4
CLE = "BYE"