Romain MARTINS
Antoine SAADA
Damien Rabier

2022

Organisation :

Pour cette SAE, nous avons décidé de coder nos différents programmes en python étant donné que grâce aux TD de Cryptographie nous avions déjà une base pour certaines méthodes de décryptage. Nous avons aussi créé un dépôt GitHub pour pouvoir mieux travailler et s'entraider au fil de la SAE.

Message n1 :

Ce message étant le premier, nous avons tester les fonctions césar et vigenère que l'on avait déjà fait en TD, aucun des deux ne marchait, donc ensuite nous sommes aller voir nos cours / TD pour voir quel méthode de cryptage on avait parler et était possiblement celle de ce message.
Nous nous sommes renseigné sur les différentes méthodes et avons testé la manière de les reconnaître, pour affine, le message chiffré a un indice de coïncidence proche de celui de la langue recherché ici français, ayant déjà la fonction d'indice de coïncidence nous l'avons testé et trouvé un rapprochement, nous sommes alors allez vérifier sur internet notre message avec le cryptage affine et avons trouvé un résultat.
Nous n'avons pas eu de réelle problème avec cette méthode là excepté un petit problème de complexité très vite réglé en changeant le fait de vérifier si

chaque mot est dans le dictionnaire à vérifier le taux d'apparition de chaque lettre dans la langue française.

Message n2 :

Pour ce deuxième message, cela a été plutôt rapide, ayant déjà commencé la fonction de vigenère en cours, nous l'avons testé sur celui-ci et trouvé un résultat, il ne nous restait plus qu'à faire la fonction qui trouve la clé automatiquement.
Cependant nous avons tout de même rencontré des problème lorsqu'il fallait trouver la longueur de la clé mais celui ci a été résolu.

Message n3 :

Pour ce message, avec notre méthode habituelle nous n'avons pas réussi à trouver un lien entre la méthode Hill et le message, après de multiples essais nous avons au final utiliser un site internet pour trouver de quel langage il s'agissait.
Pour le codage les problèmes rencontrés ont été comment gérer la ponctuation de la phrase et chercher comment trouver la clé de décodage pour au final ce rendre compte qu'il fallait utiliser la force brute (tester toutes les possibilités).
Cependant cette force brut n'a pas été concluante bien que notre cryptage est fonctionnelle, le décryptage lui ne l'est pas

Message n4 :

Ce message étant crypté en César fût très facile à trouver sachant qu'on avait déjà toutes les fonctions requises, décryptage et recherche de la clé.
Finalement, aucun problème sur celui-ci. Lorsqu'on utilise ce message avec le decryptage de Vigenère nous trouvons également un résultat convenable.

Message n5 :

Connaissant les 5 méthodes utilisées dans cette SAE, par déduction nous avons compris que ce message était codé grâce à la méthode par substitution mono-alphabétique. Nous n’avons pas réussi à finir pour l’instant ayant des problèmes avec la recherche de la clé.