Sécurité Informatique 2015-2016
L3 S6

RAPPORT

TP DE CHIFFREMENT PAR SUBSTITUTION

ACKER Edgar 21302055
DIONISIO Christopher 21302268
JACQUETTE Pierrick 21305551

César

I. Méthode mot

Pour le décryptage du code de César par un mot, on prend un mot qu'on connaît dans le texte clair et on le cherche dans le texte chiffré. Dans notre, cas on chiffre le mot qu'on cherche dans les 26 manières possibles une par une jusqu'à ce que l'on le trouve dans le texte chiffré. Si il a été trouvé, alors on essaye de déchiffrer le texte dans le décalage courant et si le texte décrypté est en français (grâce a une recherche des mots du texte dans le lexique par dichotomie), on renvoie le texte en clair, sinon on recommence la recherche du mot avec le décalage suivant. On teste si tous les mots sont dans le lexique car il existe un problème de redondance dans le code de César, par exemple le mot « grave » et le mot « tenir » sont chiffrés de la même manière avec deux décalages différents. Il faut donc faire attention a ce genre de cas ou l'on peut confondre les deux mots et donc ne pas avoir le bon décalage pour déchiffrer le texte.

II. Méthode fréquence

Pour le décryptage du code de César par la fréquence, on a recherché la fréquence des lettres en moyenne dans un texte de français. Cela nous donne un ordre d'apparition des lettres en français qu'on va utiliser pour la suite. Dans le texte chiffré, on va alors regarder le caractère le plus fréquent, puis on va supposer que c'est la lettre la plus fréquente dans notre ordre obtenue précédemment. On calcul le décalage puis on va donc tenter de déchiffrer le texte . Si il est en français, alors on le renvoie sinon, on recommence avec le caractère suivant et ainsi de suite.

III. Méthode brute

Pour la méthode brute on teste tout les décalages possible jusqu'à ce que l'on trouve le bon.

Vigenere

Pour le chiffrement et le déchiffrement, on connaît le mot clé. On parcourt en parallèle le mot clé et le texte pour créer le texte chiffré au passage. Cela ne permet de ne pas appliquer le chiffrement et le déchiffrement sur les caractères spéciaux ou les espaces mais de les conserver.

Pour le décryptage, on connaît la longueur du mot clé. Cela nous permet d'étudier la fréquence dans les sous chaînes. on récupère donc des sous-chaines où on analyse la fréquence de chaque sous-chaine, ce qui nous permet de connaître quel est le caractère pour décrypter. Une fois la clé trouvée, on applique la fonction de déchiffrement sur le texte avec la clé que l'on vient de calculer.

Le chiffre de Vigenère est un cas particulier du chiffre de César où la taille de la clé peut être supérieur à un. Utiliser la force brut pour casser ce code serait trop longue : $26^{\wedge 26}$ possibilités.

Décryptage sans clé :

Pour le décryptage de Vigenère sans clé, on cherche à connaître la longueur de la clé utilisée.

On va utiliser l'indice de coïncidence qui mesure la probabilité que dans un texte, si on prend deux lettres au hasard, alors ce sont les mêmes. On va, dans le texte, calculer la moyenne des indices de coïncidences obtenus dans tous les sous-textes (on calcule l'indice de coïncidence du texte, puis on calcule la moyenne des deux indices correspondant aux deux sous textes en prenant une lettre sur deux, etc). Si l'indice obtenu est proche de celle du français, on en déduit la longueur de la clé. On procède ensuite par analyse fréquentielle pour trouver la clé.

Permutation

Pour le chiffrement et le déchiffrement, on connaît la permutation. A chaque caractère du texte qui est compris entre « a » et « z », on applique la permutation que l'on connaît. Pour le déchiffrement, on applique la permutation inverse.

Pour le décryptage, on compte le nombre de chaque lettre dans le texte puis on se base sur la fréquence dans l'ordre décroissant des lettres françaises (e, a, s, i ...). On en déduit la permutation puis on applique la fonction de déchiffrement, cela nous donne un déchiffrement partiel. Les fréquences de certaines lettres sont assez proches, par conséquent identifier la bonne permutation est complexe.

LIGNES DE COMMANDES

Chiffre c nombre fichier
Chiffre v motCle fichier
Chiffre p permutation fichier

Dechiffre c nombre fichier
Dechiffre v motCle fichier
Dechiffre p permutation fichier

Decrypt c fichier 1 mot //mot
Decrypt c fichier 2 //frequence
Decrypt c fichier 3 //force brut
Decrypt v fichier 1 tailleMotCle
Decrypt v fichier 2
Decrypt p fichier