Projet IN 200 – Cryptanalyse et chiffrements

Par Eloïse, Lukas et Sourya

*Hello hello !*

*J’ai fait un petit résumé des consignes pour que ce que l’on doit faire soit plus clair.*

*J’ai aussi fais un mini descriptif des méthodes de chiffrements pour que l’on sache tous bien ce qu’elles sont et de quoi on a besoin pour les programmer et les attaquer.*

*Si vous trouvez qu’il manque deux trois trucs n’hésitez pas à ajouter des choses .*

*Et faites des petits commentaires*

# I - Les consignes

But

Être capable de programmer et de casser les chiffrements anciens

Compétences

* Travailler sur les longues chaine de caractères
* Ecrire et lire sur des fichiers qui sont en dehors du code python ( quelque part dans l’ordinateur)
* Programmer l’ensemble des chiffrements et déchiffrements
  + Chiffre de César
  + Chiffre de Vigenère
  + Scytale
  + Substitution monoalphabétique générale
* Programmer des attaques sur les chiffrements qui permettent grâce au code python de retrouver le texte initial sans connaitre la clef (pour tous les chiffrements)

A faire

* Programmer 8 fonctions qui chiffrent et déchiffrement en prenant en entrée le texte en clair (le message à coder, une chaine de caractère) et la clef et qui renvoient le texte chiffré
* Programmer des fonctions qui prennent en entrée le chemin du fichier contenant le texte à chiffrer ou à déchiffrer
* Programmer des attaques sur les chiffrements à partir d’un texte chiffrer mais sans connaitre la clef et retrouver tout (ou en partie) le texte initial
* Bonus : Enigma

# II – Chiffrements par substitution

* Manipulation de chaînes de caractères
  + Laisser la possibilité de supprimer les espaces ou les caractères spéciaux
  + Chiffrer un texte écrit dans un fichier .txt situé n’importe où dans l’ordinateur
  + Généraliser le code de César ou le chiffre de Vigenère à des alphabets plus grand

La substitution monoalphabétique

La substitution monoalphabétique est un procédé de cryptographie classique. Elle consiste à remplacer chaque lettre du message par une autre lettre de l'alphabet. Le chiffrement est dit monoalphabétique car il utilise un seul alphabet. Les lettres de l'alphabet sont remplacées selon une correspondance 1-1, c'est-à-dire qu'une lettre en clair correspond toujours à la même lettre chiffrée

Le chiffre de César

Le texte chiffré s'obtient en remplaçant chaque lettre du texte clair original par une lettre à distance fixe, toujours du même côté, dans l'ordre de l'alphabet. Pour les dernières lettres on reprend au début. Par exemple avec un décalage de 3 vers la droite, A est remplacé par D, B devient E, et ainsi jusqu'à W qui devient Z, puis X devient A etc.

Il s'agit d'une permutation circulaire de l'alphabet. La longueur du décalage constitue la clé du chiffrement qu'il suffit de transmettre au destinataire — s'il sait déjà qu'il s'agit d'un chiffrement de César — pour que celui-ci puisse déchiffrer le message.

Dans le cas de l'alphabet latin, le chiffre de César n'a que 26 clés possibles.

Ex : clef 3

Texte clair – bla bla bla

Texte chiffré – Ekd ekd ekd

Chiffre de Vigenère

C’est un système de chiffrement par substitution polyalphabétique dans lequel une même lettre du message clair peut, suivant sa position dans celui-ci, être remplacée par des lettres différentes.

Une clé se présente généralement sous la forme d'un mot ou d'une phrase. Pour pouvoir chiffrer le texte, chaque caractère utilise une lettre de la clé pour effectuer la substitution. Plus la clé est longue et variée, mieux le texte est chiffré.

L'outil indispensable du chiffrement de Vigenère est la « [table de Vigenère](https://haltode.fr/img/algo/chiffrement/chiffre_vigenere/table_vigenere.png) »

Pour chaque lettre en clair, on sélectionne la colonne correspondante et pour une lettre de la clé on sélectionne la ligne adéquate, puis au croisement de la ligne et de la colonne on trouve la lettre chiffrée. La lettre de la clé est à prendre dans l'ordre dans laquelle elle se présente et on répète la clé en boucle autant que nécessaire.

Mathématiquement, on identifie les lettres de l'alphabet aux nombres de 0 à 25 (A=0, B=1...). Les opérations de chiffrement et de déchiffrement sont, pour chaque lettre, celles du chiffre de César. En désignant la ieme lettre du texte clair par Texte[i], i du chiffré par Chiffré[i], et la i lettre de la clé, répétée suffisamment de fois, par Clés[i], elle se formalise par :

Chiffré[i] = (Texte[i] + Clés[i]) modulo 26

Texte[i] = (Chiffré[i] - Clés[i]) modulo 26

où x modulo 26 désigne le reste de la division entière de x par 26. Pour le chiffrement il suffit d'effectuer l'addition des deux lettres puis de soustraire 26 si le résultat dépasse 26. Pour le déchiffrement il suffit d'effectuer la soustraction et d'additionner 26 si le résultat est négatif. Le déchiffrement est aussi une opération identique à celle du chiffrement pour la clé obtenue par Clé'[i] = 26 - Clé[i]. Un disque à chiffrer (en), qui utilise une représentation circulaire de l'alphabet (après Z on a A), permet de réaliser directement cette opération.

Le chiffré d'un texte suffisamment long constitué uniquement de A donne la clé ( 0 + x = x, soit A + Clés[i] = Clés[i] ).

La Scytale

C’était un bâton de bois utilisé pour lire ou écrire un texte chiffrée. Elle permettait l'inscription d'un message chiffré sur une fine lanière de cuir ou de parchemin que le messager pouvait porter à sa ceinture.

Après avoir enroulé la ceinture sur la scytale, le message était écrit en plaçant une lettre sur chaque circonvolution. Pour le déchiffrer, le destinataire devait posséder un bâton d'un diamètre identique à celui utilisé pour l'encodage. Il lui suffisait alors d'enrouler la scytale autour de ce bâton pour obtenir le message en clair.

# III – Programmer des attaques

Attaquer César

Le chiffre de César peut être cassé très facilement :

* + soit on sait que c’est codé en César et on cherche la valeur du décalage
    - Force brute : tester toutes les combinaisons possibles de décalage
  + soit on sait pas mais on sait que s’est un chiffrement par substitution mais on sait pas lequel
    - Analyse des fréquences : si régularité dans les décalages, et en déduira que l'algorithme employé est le chiffre de César.

NB : Besoin de textes longs pour cette méthode

Décrypter Vigenère

Plusieurs modes opératoires :

* Si on connait le nombre de symboles que comporte la clé
  + - analyse de fréquences sur chacun des sous-textes déterminés en sélectionnant des lettres du message clair à intervalle la longueur de la clef (autant de sous-textes que la longueur de la clef).
  + Si on ne connait pas la longueur de la clef
    - Chercher les séquences redondantes et calculer le nombre de lettres entre les répétitions

Plus d’info [ici](https://fr.wikipedia.org/wiki/Cryptanalyse_du_chiffre_de_Vigen%C3%A8re)

Casser la scytale

C’est une variante de ceux basés sur les grilles qu'on remplit ligne par ligne avec le texte en clair : les transpositions rectangulaires. Un texte chiffré correspond aux colonnes de la grille. La taille du bâton symbolise la largeur de la grille de transposition.

Avec cette vision du chiffrement, on peut dès lors attaquer avec les étapes suivantes :

1. Compter le nombre de lettres sur la bande (ici 21)

2. Créer des grilles de plusieurs tailles de façon à pouvoir placer toutes les lettres. Avec 21, nous avons 2×11, 3×7, 4×6, 5×5, 6×4, etc.

3. Pour chaque grille, on remplit les cases ligne par ligne avec le texte chiffré. On fait de même avec une copie de cette grille mais en remplissant colonne par colonne cette fois. Cela revient à avoir par exemple une grille de 4×6 et 6×4.

4. Vérifier si un texte en clair apparaît perpendiculairement au remplissage de la grille (si on a rempli ligne par ligne, on lit colonne par colonne).

# IV – Bonus Enigma

* Programmer une version numérique de la machine