Projet IN200 - Cryptanalyse de chiffrements

Yann Rotella
yann.rotella@uvsq.fr

2023

Le but de ce projet est de programmer des algorithmes de chiffrements utilisés avant l'utilisation d'algorithmes modernes, mais surtout de programmer des algorithmes capables de "casser" ces chiffrements anciens.

Dans un premier temps, il faudra programmer en python le code de césar, le chiffre de Vigenère ainsi que la scytale, et une substitution monoalphabétique générale. Toutes les descriptions peuvent être trouvés sur internet facilement.

Pour cela, il va falloir manipuler des chaînes de caractères, on veillera à laisser la possibilité à l'utilisateur de supprimer les espaces ou les caractères spéciaux, chiffrer un texte écrit dans un fichier .txt qui se situerait n'importe où dans l'ordinateur, ou généraliser le code de César ou le chiffre de Vigenère à des alphabets plus grands.

Dans un deuxième temps, il faudra programmer des attaques (cryptanalyse) de ces trois chiffrements, en utilisant ou bien la force brute (tester toutes les clefs possibles), ou bien l'analyse de fréquence, ou la très connue cryptanalyse de Vigenère. Encore une fois, des descriptions complètes peuvent être facilement trouvées sur internet.

Enfin, les étudiant.e.s pourront essayer de trouver une description de la machine à chiffrer Enigma, et pourront programmer une version numérique de cette machine à chiffrer.

Pour conclure, dans ce projet, il faudra être capable de travailler sur de longues chaînes de caractères, écrire et lire sur des fichiers qui sont "en dehors" du code python, et programmer l'ensemble des (dé)chiffrements décrits précédemment. Ensuite, il faudra programmer les attaques sur ces chiffrements, qui permettent grâce à un code python de retrouver le texte initial sans connaître la clef et ce pour chacun de ces chiffrements. Pour terminer, les étudiant.e.s devront programmer une version numérique en python de la machine à chiffrer Enigma.

Pour commencer, des références pour ces chiffrements peuvent être trouvées sur Wikipédia :

— `https://fr.wikipedia.org/wiki/Chiffrement_par_substitution`
— `https://fr.wikipedia.org/wiki/Chiffrement_par_decalage`

— `https://fr.wikipedia.org/wiki/Scytale`
— `https://fr.wikipedia.org/wiki/Chiffre_de_Vigenere`

Il faut donc dans ce projet :

— Programmer 8 fonctions qui chiffrent et déchiffrent, qui prennent en entrée une chaîne de caractères et la clef et qui renvoient le chiffré (respectivement le message initial, le clair)
— Programmer des fonctions qui prennent en entrée un chemin dans l'ordinateur contenant le chemin du fichier contenant un texte à chiffrer ou à déchiffrer
— Programmer les attaques sur ces chiffrements : à partir d'un texte chiffré, mais sans connaissance de la clef, retrouver tout ou partie de la clef ou du message initial. On aura besoin dans certains cas d'un texte assez long.
— Bonus : on pourra programmer une version en Python de la machine à chiffrer Enigma.