Alexandre Cormier 111 101 150
Alexandre Picard-Lemieux 111 103 625
Patrick Côté 111 103 743
Vincent Beaudoin 111 103 778

Étude de la viabilité de la programmation par contraintes pour attaquer la cryptographie classique par substitution

Le chiffrement par substitution est une façon de cacher un message en remplaçant chaque lettre par une autre. On parle de substutition monoalphabétique lorsque qu'une lettre est toujours remplacée par la même autre lettre. Autrement, on parle de substitution polyalphabétique.

Un exemple de chiffrement par substitution monoalphabétique est le chiffre de César. Pour ce chiffre, on associe à chaque lettre sa position dans l'alphabet, commençant par 0. La clé est une lettre et chaque lettre du message est décalée d'un nombre de positions correspondant à la clé. Par exemple, le message `ABC` chiffré avec la clé `B` devient `BCD`. Les calculs de décalage se font en modulo 26, tel que `XYZ` chiffré avec la même clé devient `YZA`.

Le chiffre de vigenère est un exemple de chiffrement par substitution polyalphabétique. La clé est composée d'une ou plusieurs lettres et le message est placé divisé en partie de la même longueur que la clé. Si les différentes parties du message sont placées l'une en-dessous de l'autre, il suffit d'appliquer le chiffre de César à chaque colonne i avec la i^{eme} lettre de la clé. Par exemple, le message `ABCD` chiffré avec la clé `BC` devient `BDDF`.

La substition est toujours une composante à la base de la cryptographie moderne, mais ces méthodes de chiffrement simples ne sont plus utilisées comme systèmes cryptographiques à part entière puisqu'elles sont vulnérables à différentes attaques. Il est possible, notamment, d'analyser la fréquence relative des lettres dans le message chiffré et comparer avec la fréquence relative des lettres dans la langue du message d'origine pour trouver les clés les plus probables.

Dans le cadre de ce projet, nous étudierons une méthode alternative, utilisant la programmation par contrainte, pour retrouver la clé de tels chiffrements à partir du message chiffré. Il est évidemment impossible pour un programme automatisé de trouver la clé de façon certaine, car il n'y a pas nécessairement moyen de reconnaître le message d'origine lorsque la bonne clé est trouvée. Par contre, nous pourrons ordonner les clés les plus probables selon, notamment, la fréquence relative de chaque lettre dans le message déchiffré.

L'objectif ici est d'étudier la viabilité d'une telle approche, par contrainte, pour l'attaque du chiffrement par substitution. Nous étudierons l'efficacité de l'approche selon la longueur du message et, dans le cas du chiffre de Vigenère, de la longueur de la clé.

Nous pourrons aussi explorer s'il y a moyen d'appliquer cette approche efficacement sans connaître au préalable la langue du message d'origine et la longueur de la clé pour le chiffrement de Vigenère.