Université de Paris

Mathématiques discrètes
Projet : Attaque de chiffrements

Consignes Le but du projet est de présenter une application dans laquelle les mathématiques discrètes jouent un rôle fondamental.

Le rendu final du projet consistera en un article destiné au grand public au format pdf de 800-1000 mots plus une annexe numérique, qui pourra contenir par exemple une démonstration interactive, une vidéo explicative et/ou des graphiques générés par du code écrit par vous-même ; cette annexe sera rendue sous la forme d'un lien vers un dépôt en ligne. La forme exacte et la technologie utilisée pour l'annexe peut varier et est donc laissé au libre choix des étudiants. L'article et son annexe seront jugés non seulement sur le contenu mais aussi sur la clarté de la présentation, la qualité de rédaction, et la créativité.

Contenu Le sujet détaille quelques points à développer mais ceux-ci sont seulement proposés comme point de départ de votre travail. Vous êtes encouragés à développer d'autres pistes en lien avec les mathématiques discrètes. De même, la bibliographie conseillée est un point de départ. Vous pouvez vous appuyer sur d'autres sources sur lesquelles vous porterez un œil critique et que vous prendrez soin de citer correctement.

Charte de bonne conduite Lisez attentivement la charte de bonne conduite. Portez une attention particulière à citer toutes vos sources, y compris les exemples et les images que vous utiliserez. L'utilisation d'outils d'IA tels que ChatGPT est formellement interdite. L'équipe pédagogique sera très attentive à tous ces aspects lors de la correction.

Calendrier Consultez la page Moodle du cours pour les dates des principales étapes du projet.

Bref descriptif du sujet

Le projet vise à détailler des méthodes permettant de casser des systèmes de chiffrement utilisés par le passé, comme le chiffrement de César, et le chiffrement de Vigenère. Au premier siècle avant J.-C., Jules César chiffrait ses communications pendant la guerre des Gaules à l'aide de l'algorithme suivant : il décalait chaque lettre de trois crans dans l'alphabet (A devient D, B devient E, etc.). Le chiffrement de Vigenère est une généralisation plus résistante du chiffrement de César, utilisant un décalage dit *poly-alphabétique*.

Bibliographie conseillée

- `https://fr.wikipedia.org/wiki/Chiffrement_par_d%C3%A9calage`
- `https://fr.wikipedia.org/wiki/Chiffre_de_Vigen%C3%A8re`
- `https://fr.wikipedia.org/wiki/Cryptanalyse_du_chiffre_de_Vigen%C3%A8re`
- `https://www.apprendre-en-ligne.net/crypto/vigenere/decodevig.html`

Pistes de développement

1. Détailler les principes de l'analyse fréquentielle
2. Écrire un programme permettant à un utilisateur de chiffrer un message clair avec le procédé de Vigenère
3. (Plus difficile) implémenter une méthode qui détermine, à partir d'un texte chiffré, une clé probable
4. Établir la formule de l'indice de coïncidence