Université de Paris

Mathématiques discrètes
Projet : Énigme des 100 prisonniers

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

L'énigme des cent prisonniers est une énigme célèbre proposée en 2003 par l'informaticien danois Peter Bro Miltersen. En voici l'énoncé :
Cent prisonniers ont été condamnés à mort. Néanmoins, le directeur de la prison a décidé de leur offrir une ultime chance de s'en sortir : chaque prisonnier se voit affecter un nombre unique, entre un et cent. Ensuite, les cent numéros sont placés dans cent tiroirs, au centre d'une pièce. Un par un, les prisonniers sont amenés dans cette pièce, et sont autorisés à ouvrir cinquante tiroirs. La pièce est remise en l'état après chaque passage d'un prisonnier, et les prisonniers ne peuvent pas communiquer entre eux entre chaque passage (mais ils peuvent établir une stratégie avant le début de l'épreuve). Le directeur annonce que les prisonnier seront libérés, mais uniquement s'ils réussissent *tous sans exception* à trouver leur numéro parmi les cinquante boîtes qu'ils auront ouvertes. Quelle est la stratégie que doivent adopter les prisonniers pour maximiser les chances de s'en sortir, et quelle est la probabilité qu'ils s'en sortent ?

De façon très surprenante, la bonne réponse n'est pas $1/2^{100}$, mais... près de 30%. Pour le démontrer, il faut s'intéresser à un objet combinatoire : les graphes de permutation. Un graphe de permutation à N noeuds est un graphe orienté avec N arêtes qui représente une permutation P de $\{1, ..., n\}$, où une arête d'un sommet i vers un sommet j indique que $P(i) = j$. La question de combinatoire à se poser est la suivante : quelle est la probabilité que le graphe d'une permutation aléatoire ne possède aucun cycle de longueur strictement supérieure à 50 ?
Cette énigme est en fait une illustration élégante d'un algorithme fondamental : le *baby-step giant-step* ("pas de bébés, pas de géants"). Cet algorithme est au cœur de la méthode générique d'attaque de systèmes de chiffrement basés sur le logarithme discret, l'un des deux grands systèmes de chiffrement (avec RSA) utilisé partout dans le monde aujourd'hui.

Bibliographie conseillée

- `https://cristal.univ-lille.fr/~jdelahay/pls/272.pdf`
- `https://en.wikipedia.org/wiki/100_prisoners_problem` (attention, page en anglais n'existant pas en version française)
- `https://fr.wikipedia.org/wiki/Baby-step_giant-step`
- `http://defeo.lu/in420/Pas%20de%20b%C3%A9b%C3%A9%20et%20pas%20de%20g%C3%A9ant#:~:text=L'algorithme%20pas%20de%20b%C3%A9b%C3%A9,une%20occupation%20de%20m%C3%A9moire%20accrue.`

Pistes de développement

1. Décrire proprement la résolution de l'énigme des cent prisonniers.
2. Établir la formule permettant de calculer la probabilité qu'une permutation aléatoire de N entiers contienne un cycle de longueur au moins k.
3. Écrire un programme permettant au lecteur de tester l'énigme des cent prisonniers. Programmer la stratégie gagnante, afin de montrer qu'elle fonctionne bien environ 30% du temps.
4. Écrire un programme qui représente le graphe d'une permutation.
5. Écrire un programme qui trouve tous les cycles d'une permutation, et vérifier expérimentalement la formule pour de petites valeurs de N et k.
6. Décrire l'application de l'énigme des cent prisonniers à l'attaque de schémas cryptographiques basés sur le logarithme discret à partir de l'algorithme baby-step giant-step.