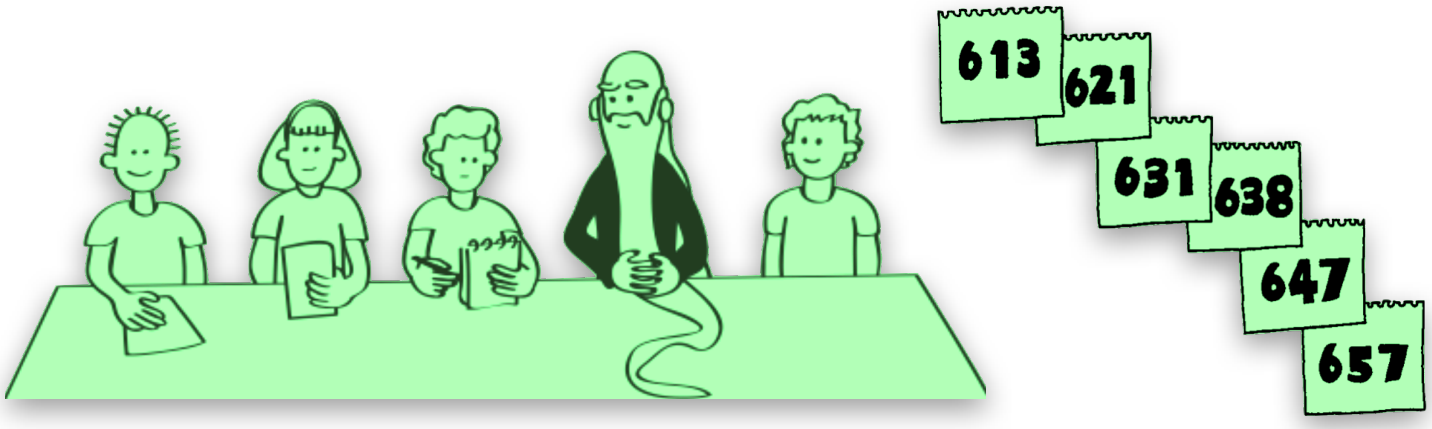
Chapitre 5 - Section 1
Partager des secrets

1



Protocoles de masquage des données

Les techniques cryptographiques permettent de partager des données avec d'autres personnes tout en garantissant un niveau de confidentialité étonnamment élevé. Dans cette activité, nous allons partager des informations sans rien révéler de leur contenu : chaque groupe d'élèves calculera son âge moyen sans qu'aucun des membres ne divulgue son âge.

Liens pédagogiques

- Mathématiques : sommes et moyennes

Compétences

- Calculer une moyenne
- Nombres aléatoires
- Coopération

Âge

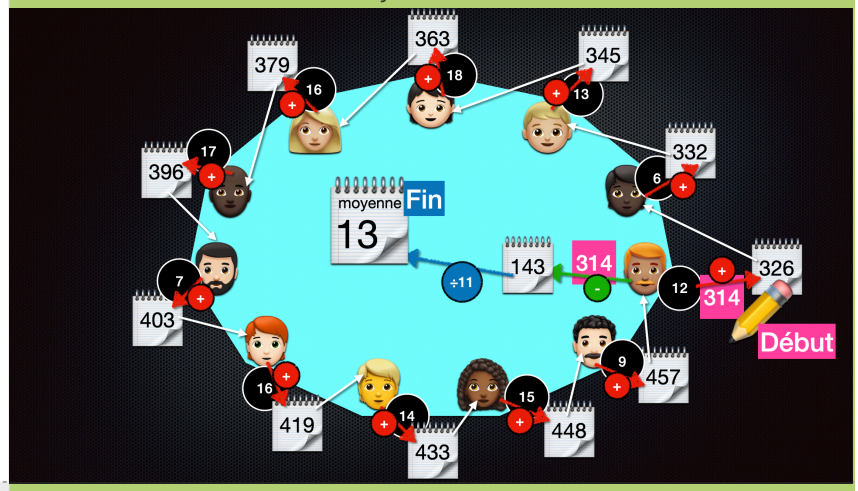
- 7 ans et plus

Matériel

- Pour chaque élève :
  - Un petit bloc-notes
  - Un stylo

Étape	Instruction	Réponse
1	Présenter la situation : Les élèves veulent la moyenne de la classe des notes du dernier devoir de mathématiques (ou autre discipline) sans qu'aucun élève ne révèle sa note à aucun autre élève.	Faites des proposition avec une liste du matériel (non numérique) nécessaire.
2	Si une méthode complète a été proposée, elle doit être testée (si besoin avec de fausses informations, pour la vérification).	
3	On propose si besoin la méthode de l'enseignant	
4	On teste. Vérification des défauts et avantages de ce protocole.	
5	Rédaction des grands principes mis en œuvre et applications dans la vie réelle.	

Correction – Chapitre 5 – Section 1

Étape	Instruction	Réponse
1	Présenter la situation : Les élèves veulent la moyenne de la classe des notes du dernier devoir de mathématiques (ou autre discipline) sans qu'aucun élève ne révèle sa note à aucun autre élève.	Faites des proposition avec une liste du matériel (non numérique) nécessaire.
2	Si une méthode complète a été proposée, elle doit être testée (si besoin avec de fausses informations, pour la vérification).	
3	On propose si besoin la méthode de l'enseignant	Le premier élève choisit un nombre aléatoire (rose) à 3 chiffres. Il note ce nombre. Il écrit la somme de ce nombre de sa note de math sur un papier qu'il donn à son voisin. Son voisin fait la somme de ce nombre et de sa propre note de math sur un papier qu'il passe à son voisin. Etc. Le dernier élève fait de même vers le premier. Celui-ci peut alors retrancher le nombre aléatoire noté au début, diviser par le nombre d'élèves et ainsi obtenir la moyenne. 
4	On teste. Vérification des défauts et avantages de ce protocole.	Si le protocole est fiable au niveau du résultat et de la confidentialité, il n'est pas à l'abri d'une erreur de protocole, de calcul ou même de « tricherie ».
5	Rédaction des grands principes mis en œuvre et applications dans la vie réelle.	Les ordinateurs stockent beaucoup de données personnelles : l'état de notre compte en banque, les impôts à payer, l'année d'obtention de notre permis de conduire, nos antécédents de crédit, nos résultats aux examens, nos dossiers médicaux, etc. Les atteintes à la vie privée sont encore assez largement acceptées, pourtant certains protocoles permettent d'effectuer des transactions financières électroniques en garantissant le même niveau de confidentialité qu'avec de l'argent liquide. Cela peut paraitre difficile à comprendre, mais il est possible de transférer de l'argent depuis son compte en banque vers celui du magasin sans que personne ne sache d'où vient l'argent ni où il va. Cette activité permet de mieux comprendre comment cela est possible : dans les deux situations, il s'agit de limiter le partage d'informations à l'aide d'un protocole ingénieux.