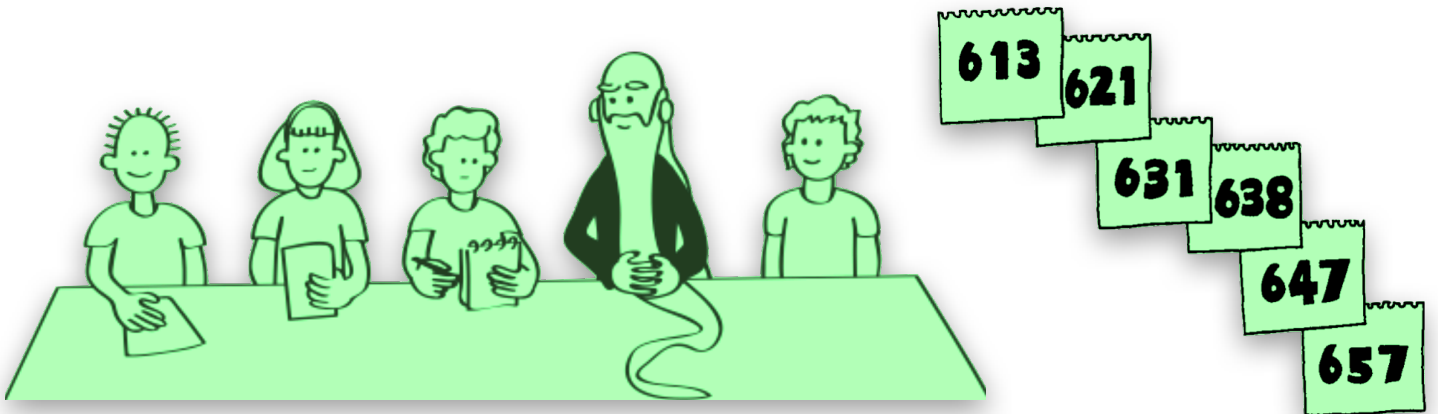


Chapitre 5 - Section 1

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


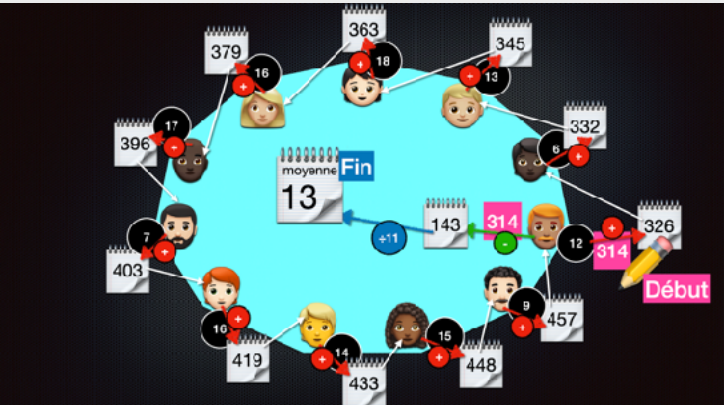
Âge

- 7 ans et plus

Matériel

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

Chapitre 5 - Section 1

Étape	Instruction	Réponse
1	Présentation de l'histoire très rapide de la cryptographie.	
2	Présenter la situation : Les participants veulent calculer la moyenne de leurs âges/salaires/notes de leur dernier devoir de mathématiques sans qu'aucun participant ne révèle sa note à aucun autre participant.	Matériel nécessaire ? Explication du protocole
3	Si une méthode complète a été proposée, elle doit être testée (si besoin avec de fausses informations, pour la vérification).	
4	On propose si besoin la méthode du formateur : Constitution de la chaîne de communication	<p>Le premier participant choisit un nombre aléatoire (rose) avec un chiffre de plus que la donnée à « partager ».</p> <p>Il note ce nombre. Dans le chat privé, il envoie la somme de ce nombre et de la données à partager à son voisin.</p> <p>Son voisin fait de même.</p> <p>Le dernier participant fait de même vers le premier. Le premier peut alors retrancher le nombre aléatoire noté au début, diviser par le nombre de participant et ainsi obtenir la moyenne.</p> 
5	On teste. Vérification des défauts et avantages de ce protocole.	Le protocole, même s'il est bien exécuté, n'empêche pas les erreurs de calcul ou les « triches ».
6	Rédaction des grands principes mis en œuvre et applications dans la vie réelle.	Stratégie du noyage de poisson et de cohérence des données. Si la protection des données est un sujet central de la vie numérique actuelle, elle a de nombreux impacts sur la vie privée, entre les informations bancaires, médicales, scolaires. Et la balance avec les possibilités légales des états ou d'autres organismes publics ou privés est en constant débat politique, économique voire philosophique.