Chapitre 5 - Section 3
Le chiffrement à clé publique

4

Chiffrement à clé publique

Le chiffrement est la clé de la sécurité de l'information. Et la clé du chiffrement moderne réside dans le fait qu'en utilisant uniquement des informations publiques, un expéditeur peut cadenasser son message de sorte qu'il ne puisse être ouvert (en privé, bien sûr) que par le destinataire prévu.

Liens pédagogiques

- Mathématiques : sommes
- Technologie : chiffrement à clé publique, codes secrets

Compétences

- Résolution d'énigmes

Âge

- 11 ans et plus

Matériel

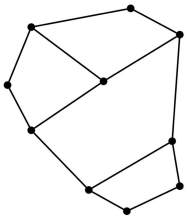
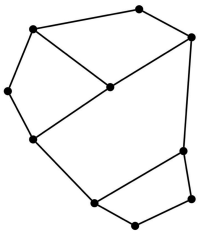
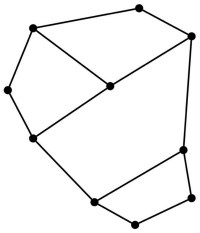
La classe est répartie en groupe d'environ quatre élèves, eux-mêmes divisés en deux sous-groupes. Chaque sous-groupe reçoit une copie de deux cartes de la fiche d'activité.

Pour chaque groupe d'élèves, il faudra donc :

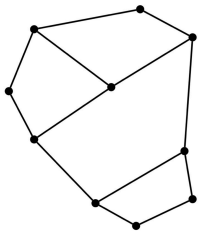
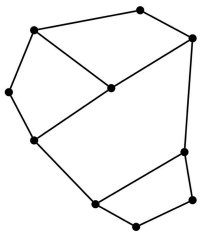
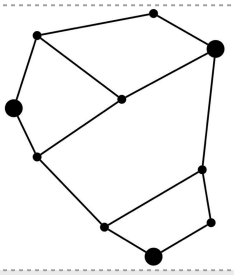
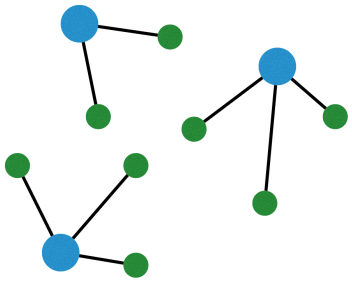
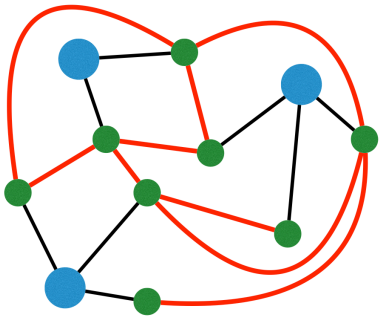
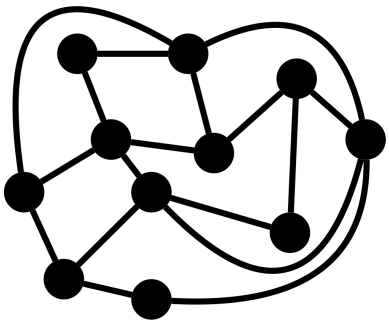
- Deux copies de la fiche d'activité *L'encodage des cryptographes en herbe*
- Des crayons
- Des calculatrices pour accélérer les calculs si besoin

Pour l'enseignant :

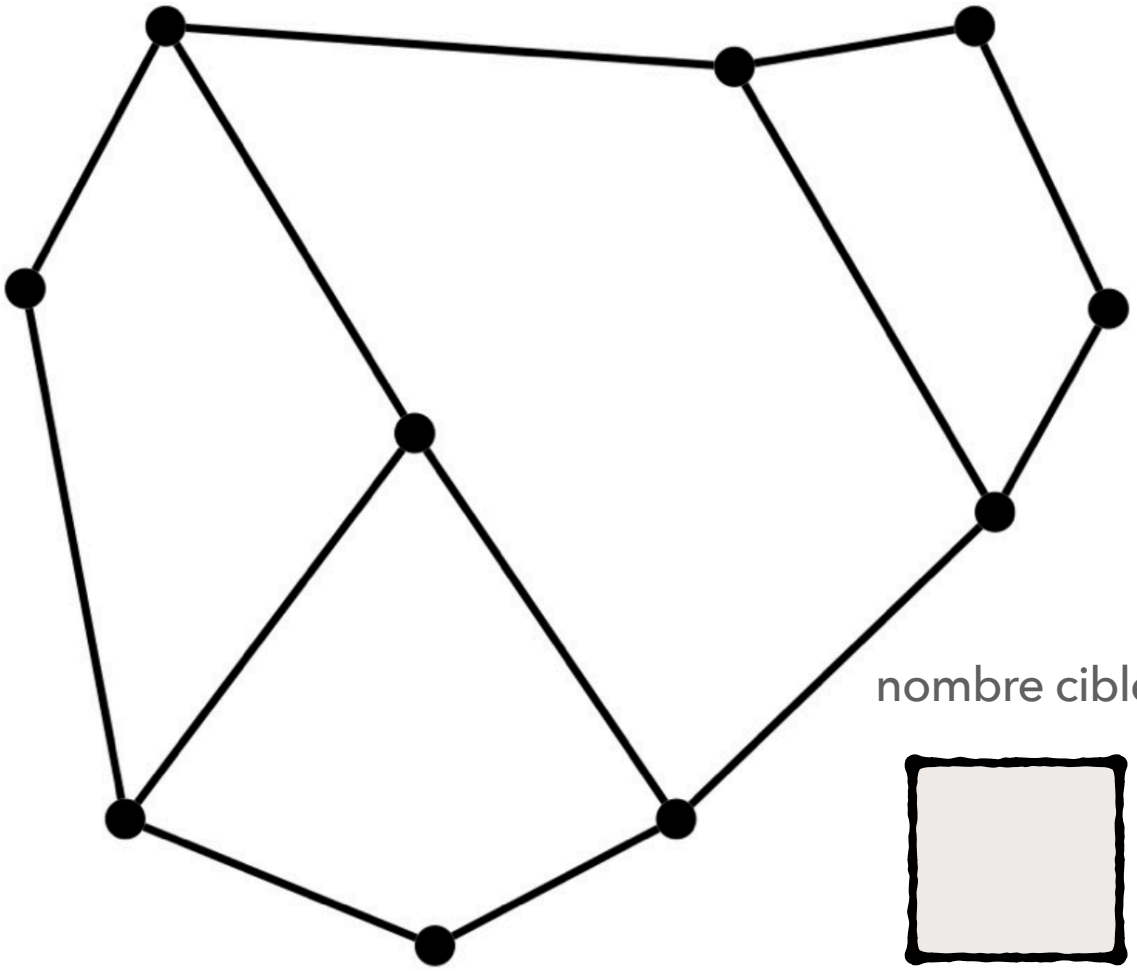
- Une projection de la fiche d'activité *L'encodage des cryptographes en herbe*
- De quoi annoter le schéma

Étape	Instruction	Réponse		
1	Présenter la situation : L'objectif est d'envoyer un message chiffré constitué d'une lettre (ou d'un nombre) avec une clé que tout le monde connait.	Explications de la clé publique :		
2	Les élèves choisissent une lettre (ou un nombre) et le chiffre sur une feuille de calcul. Ils donnent la feuille chiffrée à l'enseignant.	Lettre ou nombre choisie :		
3	L'enseignant retrouve la lettre (ou le nombre) chiffrée	Comment fait-il ?		
4	Les élèves se regroupent par 4 : par 2, ils inventent une clé privée, créent la clé publique (ou reprennent celles de l'enseignant) et donnent cette dernière aux 2 autres. Ils testent l'envoi et la réception de messages.	Lettre choisie et clé publique :	Message chiffré :	
		Message reçu et clé privée :	Message déchiffré :	

Correction Chapitre 5 - Section 3

Étape	Instruction	Réponse	
1	Présenter la situation : L'objectif est d'envoyer un message chiffré constitué d'une lettre (ou d'un nombre) avec une clé que tout le monde connait.	Explications de la clé publique : mettre des nombres sur chaque noeud pour atteindre une somme correspondante au nombre que l'on veut chiffrer sur le graphe « Message ». Sur le graphe « Message chiffré », sur chaque noeud faire la somme du noeud et de ses voisins. Découper le message chiffré et le transmettre.	
2	Les élèves choisissent une lettre (ou un nombre) et le chiffre sur une feuille de calcul. Ils donnent la feuille chiffrée à l'enseignant.	Lettre ou nombre choisie : en cas d'erreur de l'enseignant, vérifier de probables erreurs de calcul.	
3	L'enseignant retrouve la lettre (ou le nombre) chiffrée	Comment fait-il ? Il utilise les 3 noeuds principaux de sa clé privée correspondant à la clé publique. Fait la somme et retrouve le nombre du message.	
4	Les élèves se regroupent par 4 : par 2, ils inventent une clé privée, créent la clé publique (ou reprennent celles de l'enseignant) et donnent cette dernière aux 2 autres. Ils testent l'envoi et la réception de messages.	Prendre 3 ou 4 points principaux. Leurs ajouter chacun 2-3 points secondaires.	Relier autant de fois que l'on veut des points secondaires à d'autres point secondaires des autres ilots : clé privée
			
		Anonymiser le graphe pour obtenir la clé publique :	

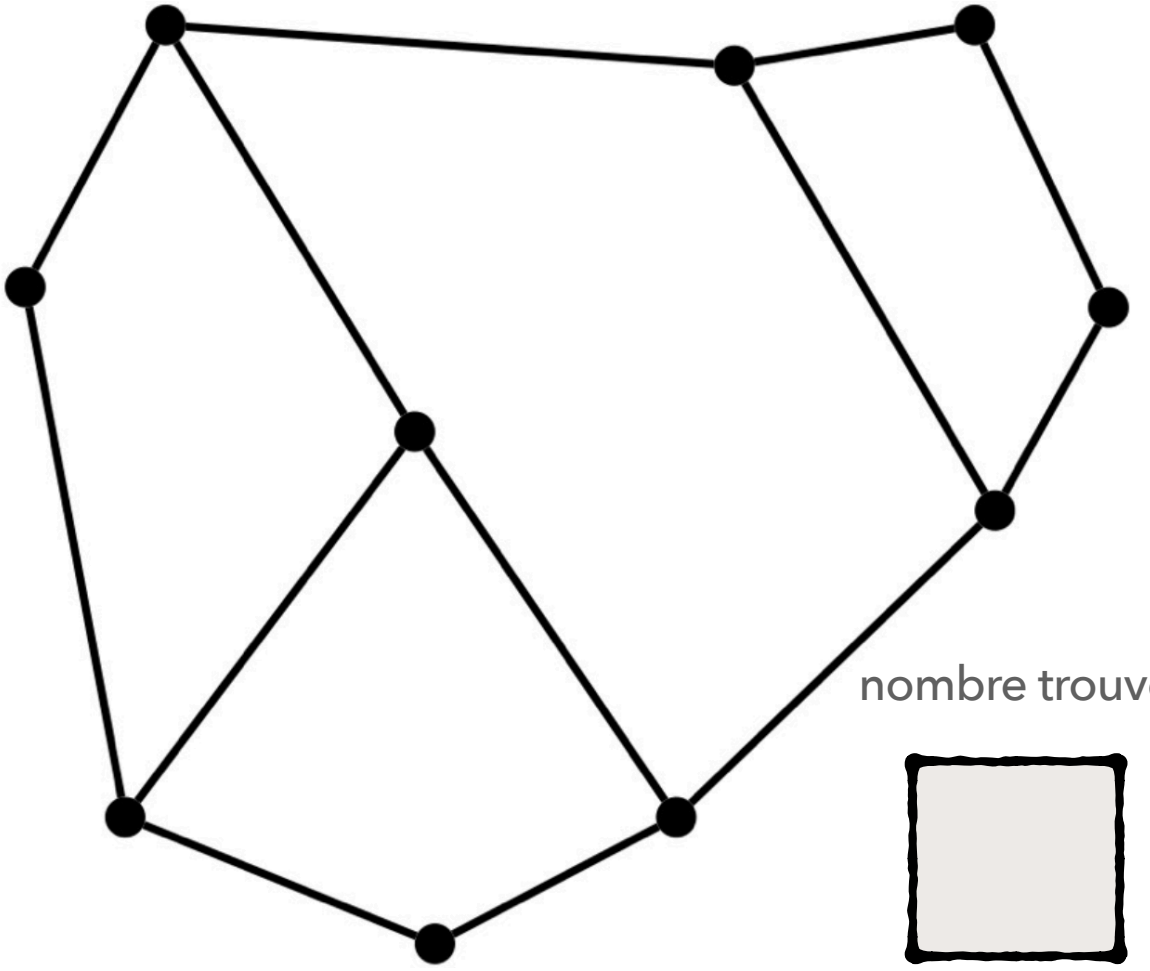
Expéditeur :



nombre cible

Message

Destinataire :



nombre trouvé

Message chiffré

Propriétaire :

Clé privée

Destinataire :

Clé publique