Chapitre 5 - Section 3
Le chiffrement à clé publique

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

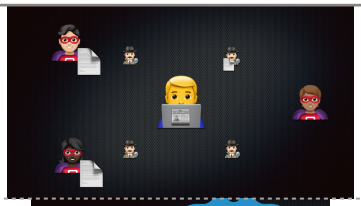
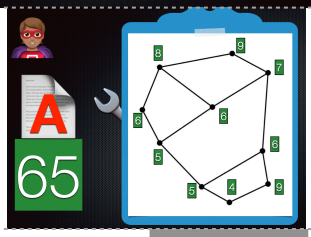
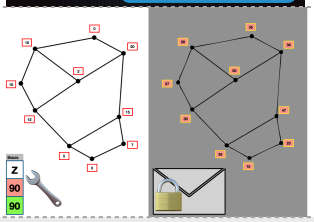
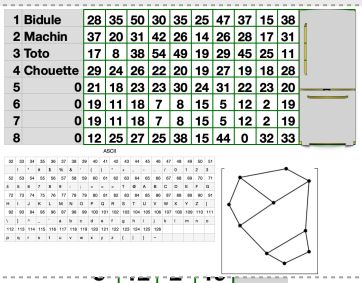
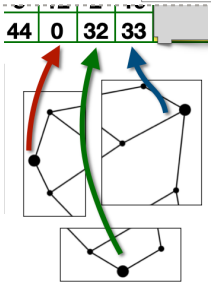
- Résolution d'énigmes

Âge

- 11 ans et plus

Matériel

- Diaporama de mise en situation
- Tableur support de l'activité : https://www.icloud.com/numbers/040lIbiiN1eByUPUDGtlKcdXw

Étape	Instruction	Réponse
1	Diaporama de présentation de la situation	
2	Présentation de la clé publique	
3	Présentation du tableur de support de l'activité	
4	Action des participants	Chaque participant s'inscrit dans le tableau d'accueil et ouvre l'onglet correspondant. Il entrent une lettre dans dans la case blanche sous leur pseudo. Ils obtiennent une valeur à atteindre (code ASCII). Ils remplissent les cases blanches du graphes pour atteindre cette valeur, la case se colorie alors en vert pour valider.
5	Action du présentateur	Lorsque tous les participants ont le feu vert, le présentateur demande aux autres s'ils peuvent deviner la lettre de chacun avec les valeurs du tableau (normalement non). Grâce à un petit calcul mental sur les 3 dernières colonnes, il devine les lettres et dévoile en déplaçant le cache réfrigérateur. 
6	Explications	Ils dévoile alors la construction de la clé publique à l'aide de la clé privée. 
7	Parole ouverte aux participants	Les participants peuvent alors proposer des failles au système (10 équations à 10 inconnues). Le présentateur parle de la non réversibilité qui ne permet alors pas de signer les messages, contrairement au RSA.
8	Explications	Retour au diaporama pour donner les explications sur le RSA, puis questions ouvertes.