ACT2 Symétrie / Asymétrie

Compétences travaillées :

APP	• Identifier les enjeux et responsabilités sociétaux induits par un usage précis du numérique
REA	• Concevoir, décrire une solution algorithmique en réponse à un problème

Dans les méthodes de chiffrement, on parle de "chiffrement à **clé symétrique**" (ou chiffrement symétrique) pour une méthode utilisant la même clé pour chiffrer et déchiffrer le message.
Imaginons qu'Alice souhaite envoyer un message à Bob, pour cela il dispose d'une clé de chiffrement symétrique de sa composition nommée KEY :

- **message** = *"Bonjour Bob, voilà ton code de CB"*
- **clé** = KEY

1) Donner des exemples de chiffrements symétriques, déjà vus ou pas.
2) Expliquer les grandes lignes du processus avec cette clé symétrique.
3) Quelles seraient les failles possibles... ?

2. Transmettre de façon sécurisée

Vous disposez du matériel :

- 2 cadenas et leur clés respectives
- 1 boîte

TRAVAIL DEMANDE

1) Trouver un moyen sécurisé de transmettre un message de Alice vers Bob.
2) Le mettre en oeuvre et faire un schéma récapitulatif des échanges.
3) Discuter des limites de cette méthode.

3. Une nouvelle faille… ?

Après avoir évoqué les limites de la méthode précédente, voivi une autre méthode plus avantageuse proposée, en suivant quelques règles :

- Alice et Bob disposent chacun d'une **clé privée** et d'une **clé publique**.
- Les **clés publiques** sont visibles et connues de tous sur le réseau, et les **clés privées** ne sont connues que de leurs propriétaires respectifs.
- La **clé publique** est symbolisée par le cadenas ouvert, et la **clé privée** est la clé du cadenas.
- L'action de chiffrer un message se fait à l'aide la **clé publique** : cela revient à fermer le cadenas.
- L'action de déchiffrer un message se fait à l'aide de la **clé privée** : cela revient à ouvrir le cadenas avec la (bonne) clé.

TRAVAIL DEMANDE

1) Mettre en place cette méthode pour transmettre un message de Alice vers Bob.
2) Faire un schéma récapitulatif des échanges.
3) Expliquer pourquoi on parle de chiffrement asymétrique pour ces deux dernières méthodes