ACTIVITÉ 2 - ECHANGES

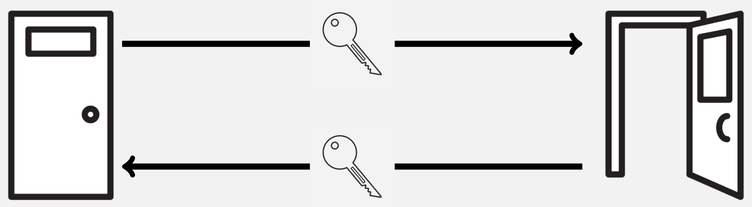
Antoine Douteau[1]
[1]Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, 14000 Caen, FRANCE
[1]en thèse dirigée par Adeline Roux-Langlois
antoine.douteau@unicaen.fr

GREYC
Laboratoire de recherche en sciences du numérique

Activité 2.1

Le chiffrement symétrique

On appelle **chiffrement symétrique** les algorithmes de chiffrement où la clé sert à la fois à chiffrer et à déchiffrer.
On peut voir ça comme la serrure d'une porte où la clé sert à la fois à verrouiller et à déverrouiller.



Pour représenter cette action, on utilisera des cadenas et des boîtes en bois. Notre algorithme de chiffrement sera alors les actions suivantes :
- écrire le message sur un papier,
- le mettre dans une boîte,
- fermer la boîte avec le cadenas.

On déchiffre le message en ouvrant la boîte.

A vous de jouer :
- **Situation 1 :** Avec 1 boîte, 1 cadenas et 2 clés, montrer comment 2 personnes peuvent s'échanger des messages de manière sécurisée.
- **Situation 2 :** Avec 1 boîte, 2 cadenas avec 1 clé chacun·e, montrer comment 2 personnes peuvent s'échanger des messages de manière sécurisée. Cette fois, chaque personne possède un unique cadenas avec une unique clé associée, et il est interdit de prêter sa clé et d'essayer d'ouvrir un cadenas qui n'est pas le sien.
- Faites la même chose pour 3 personnes.

Activité 2.2

Le chiffrement asymétrique

On appelle **chiffrement asymétrique** les algorithmes de chiffrement où la clé est séparée en deux parties. Une partie est **publique** et sert à chiffrer les messages. Une deuxième partie est **privée** et va servir à déchiffrer les messages chiffrés grâce à la clé publique associée.
On peut voir ça comme une boîte aux lettres. N'importe qui peut envoyer des messages, mais il n'est possible d'ouvrir la boîte qu'avec la clé.

A vous de jouer :
Dans un cas un peu plus proche de la réalité, considérons que chaque personne possède un unique cadenas avec une unique clé, et qu'il est interdit de prêter sa clé. En groupe, et en vous aidant du matériel présent, montrer comment 2 personnes peuvent arriver de la **Situation 2** à la **Situation 1** (c'est-à-dire communiquer avec un unique cadenas).