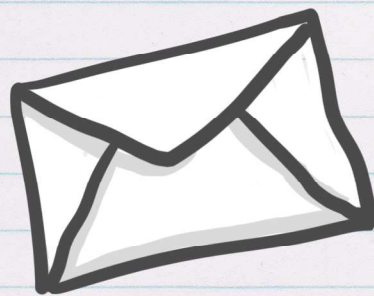


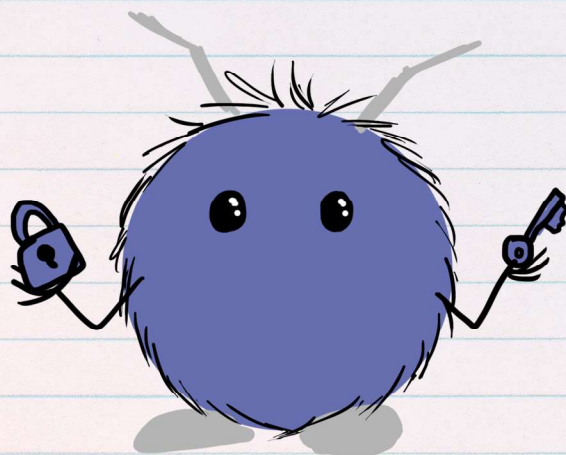
# ÉCHANGE SECRET





Avec l'atelier précédent, tu as découvert qu'il existe des méthodes pour **protéger** les échanges de messages. Mais pour cela, il faut que le destinataire connaisse la clé. Cette clé est **secrète** et ne doit pas être donnée à n'importe qui... Aide Buggy à trouver comment partager un secret !

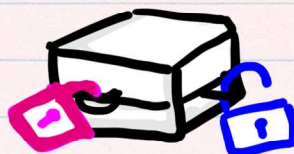
## Contexte :

**Alice** veut envoyer un **secret** à **Bob**,  
**Eve** transporte tous les messages  
échangés, mais ne doit pas découvrir  
le secret d'**Alice**.



**Alice** et **Bob** ont chacun un cadenas  et une clé.   
La clé d'**Alice** ouvre uniquement le cadenas d'**Alice**, et la clé de  
**Bob** ouvre uniquement le cadenas de **Bob**.

**Alice** a également une boîte qui peut être fermée avec un ou deux  
cadenas pour transporter le message.



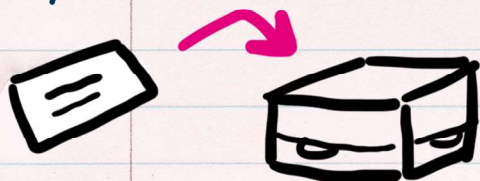


## ÉCHANGE SECRET

Buggy te propose plusieurs scénarios. Analyse chacun d'entre eux, est-ce que **Bob** connaît le secret d'**Alice** à la fin ? Est-ce que **Eve** a pu le voir durant l'échange ?

Scénario 1 :

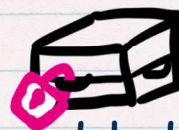
**Alice** met le secret dans la boîte, et l'envoie.



**Eve** transmet la boîte à **Bob**.

Scénario 2 :

**Alice** met le secret dans la boîte, la ferme avec son cadenas et l'envoie.



**Eve** transmet la boîte à **Bob**.

Scénario 3 :

**Alice** met le secret dans la boîte, la ferme avec son cadenas. Elle envoie la boîte et sa clé.



**Eve** transmet la boîte et la clé d'**Alice** à **Bob**.



## ÉCHANGE SECRET

Buggy te propose plusieurs scénarios. Analyse chacun d'entre eux, est-ce que **Bob** connaît le secret d'**Alice** à la fin ? Est-ce que **Eve** a pu le voir durant l'échange ?

Scénario 4 :

On essaye avec le cadenas de **Bob** :

**Alice** envoie la boîte vide.

**Eve** transmet la boîte à **Bob**.

**Bob** ferme la boîte avec son cadenas, et la renvoie.

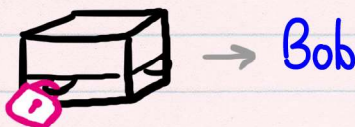


**Eve** transmet la boîte à **Alice**.

Scénario 5 :

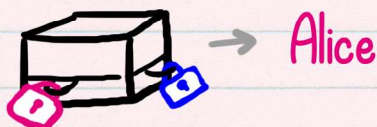
**Alice** met le secret dans la boîte, la ferme avec son cadenas et l'envoie.

**Eve** transmet la boîte à **Bob**.



**Bob** ajoute son cadenas sur la boîte et la renvoie.

**Eve** transmet la boîte à **Alice**.



**Alice** enlève son cadenas de la boîte, et la renvoie.

**Eve** transmet la boîte à **Bob**.





## ÉCHANGE SECRET

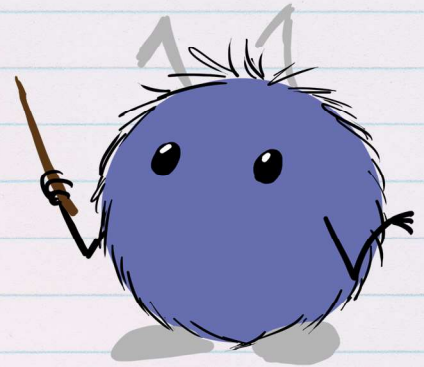
Correction

Scénario 1 :

La boîte n'est pas fermée, tout le monde a pu lire le secret.  
Il faut donc utiliser les cadenas pour protéger le secret.

Scénario 2 :

La boîte est fermée, Bob et Eve n'ont pas la clé d'Alice, personne n'a pu lire le secret.



Scénario 3 :

Bob peut utiliser la clé d'Alice pour lire le message, mais Eve aussi. Il est très dangereux d'envoyer la clé, Eve pourrait en faire un double et s'en servir plus tard par exemple.  
Il faut alors utiliser le cadenas de Bob...

Scénario 4 :

Dans ce cas, Alice ne peut pas ouvrir le cadenas de Bob pour mettre le secret dans la boîte. On s'approche de la solution !

Scénario 5 :

Eve n'a pas pu voir le secret, car la boîte est toujours fermée par au moins un cadenas quand elle la transmet.  
A la fin, Bob peut lire le secret car la boîte est fermée avec son propre cadenas.  
Ce scénario fonctionne !

