La Cryptographie Visuelle

https://dpt-info-sciences.univ-rouen.fr/index.php

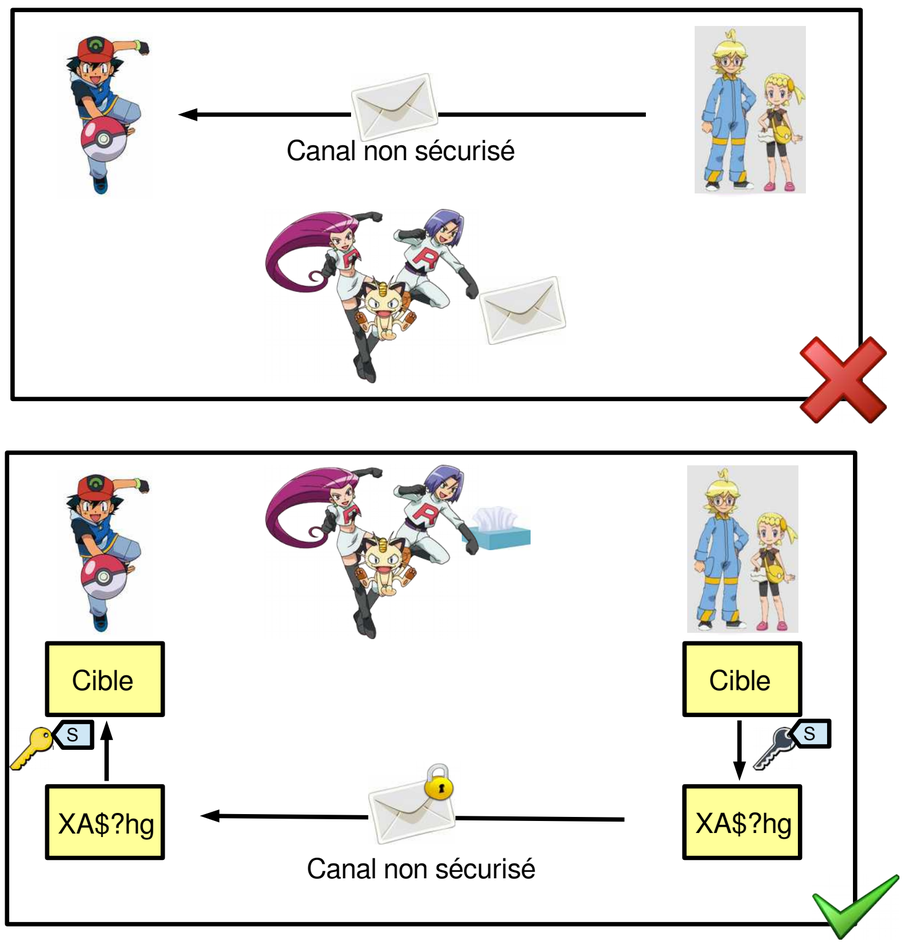
Pourquoi ?

La cryptographie permet d'assurer

- **La confidentialité des donnés :** seul le destinataire est capable de lire le message. Si un espion écoute la communication, alors il ne pourra pas retrouver le message d'origine.
- **L'authentification :** le destinataire a la garantie de l'identité de l'émetteur du message. Ainsi, un espion qui écoute la communication ne peut pas se faire passer pour l'émetteur du message.
- **L'intégrité des données :** le destinataire a la garantie que les données n'ont pas été modifiées. Ainsi, un espion qui écoute la communication ne peut pas substituer le message.

La **confidentialité** est assurée par le **chiffrement** des données.

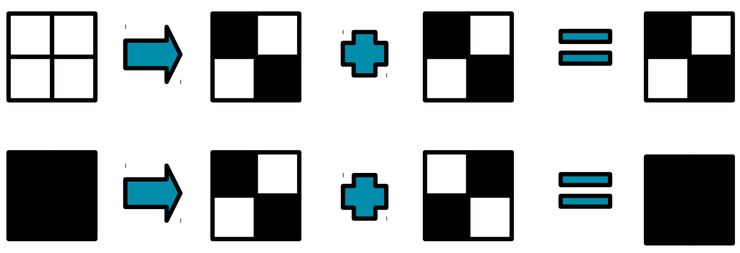
Clem et Lem veulent envoyer le pokemon que Sacha doit attraper de manière secrète.
Comment font-elles ?



Comment ça marche ?

Sur une image en **noir et blanc**, chaque pixel est découpé en 4 sous-pixels. Pour chiffrer, on divise chaque pixel (groupe de 4 sous-pixels) en deux couches avec **exactement deux sous-pixels noirs et deux sous-pixels blancs** par couche :

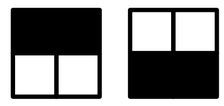
- **pixel blanc** : partagé en deux couches **identiques**
- **pixel noir** : partagé en deux couches **complémentaires**



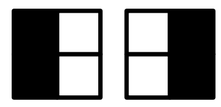
Sécurité

Pour assurer la **sécurité** de ce schéma, on ne prend pas toujours le même découpage (▚) mais on choisit un découpage **aléatoirement** parmi les 6 possibilités suivantes :

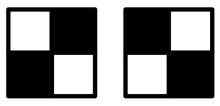
- découpage horizontal :



- découpage vertical :



- découpage diagonal :



Exemple