FICHE ENSEIGNANT

SÉCURITE DES DONNÉES

INTRODUCTION

Nous partageons toute sorte de contenus sur Internet : données privées, numéros bancaires, informations confidentielles… Si ces renseignements devaient tomber entre les mains de personnes malintentionnées, les conséquences seraient graves, voire catastrophiques dans certains cas. Pour éviter les problèmes et protéger notre identité, les données sont envoyées de façon cryptée : seule la personne destinataire des données peut les lire. Il est important de comprendre comment cela fonctionne. Parmi toutes les techniques permettant de chiffrer des messages, cette activité aborde celle du cryptage à clé publique et explique simplement son principe.

UN MÉTIER DU NUMÉRIQUE

Expert-e en sécurité informatique...

L'enseignant-e introduit l'activité en annonçant que la classe va travailler sur la sécurité des données. Il invite les élèves à découvrir la "vidéo métier" de l'experte en sécurité informatique (sur le site : *www.clesdunumerique.com*) et leur demande de réfléchir à la question : " Comment peut-on cacher des secrets sur Internet ? "

Outre la découverte d'un métier du numérique pouvant susciter la curiosité et l'intérêt des élèves, cette introduction peut leur permettre de formuler collectivement des débuts de réponses, qui seront affinées au cours de l'activité.

Bonjour, je suis expert en sécurité informatique.
Je protège les informations des entreprises. Je traque leurs points faibles pour les protéger des attaques et garantir une sécurité maximale de leurs données. D'ailleurs à votre avis, comment peut-on cacher des secrets sur Internet ?

COMPÉTENCES – LIENS AVEC LE PROGRAMME

Les méthodes et outils pour apprendre

Organisation du travail personnel :
- Identifier un problème et s'engager dans une démarche de résolution
- Analyser et exploiter les erreurs, mettre à l'essai plusieurs solutions

Coopération et réalisation de projets :
- Travailler en équipe et s'engager dans un dialogue constructif

Outils numériques pour échanger et communiquer :
- Comprendre la différence entre sphères publique et privée.
- Savoir ce qu'est une identité numérique et être attentif aux traces qu'on laisse.

FICHE ENSEIGNANT

MATÉRIEL

- Une boîte à deux serrures
- Un jeu de 2 cadenas avec leurs clés

DÉROULEMENT DE L'ACTIVITÉ

Échanger des informations privées sur Internet pose un problème très particulier : il faut que deux personnes, qui ne se connaissent peut-être pas, qui ne peuvent communiquer que publiquement devant tout le monde, donc sans s'envoyer aucune information privée, puissent tout de même s'envoyer un message secret qu'elles seules pourront lire. C'est possible, mais comment ça marche ?

Cette activité permet aux élèves de se construire une représentation de la façon dont sont chiffrés les messages. Elle permet également d'introduire la notion de protection de données personnelles.

Jeu de la boîte à cadenas

Mise en situation

Exemple : je veux acheter directement en ligne un livre sur le site Internet de mon libraire. Je dois donc envoyer le code de ma carte bleue à mon libraire. Cependant ce message est confidentiel et je veux que personne d'autre que lui ne voie ni ce que je lui envoie ni sa réponse.

La classe est divisée en trois groupes : celui de l'acheteur, celui du libraire et les espions.

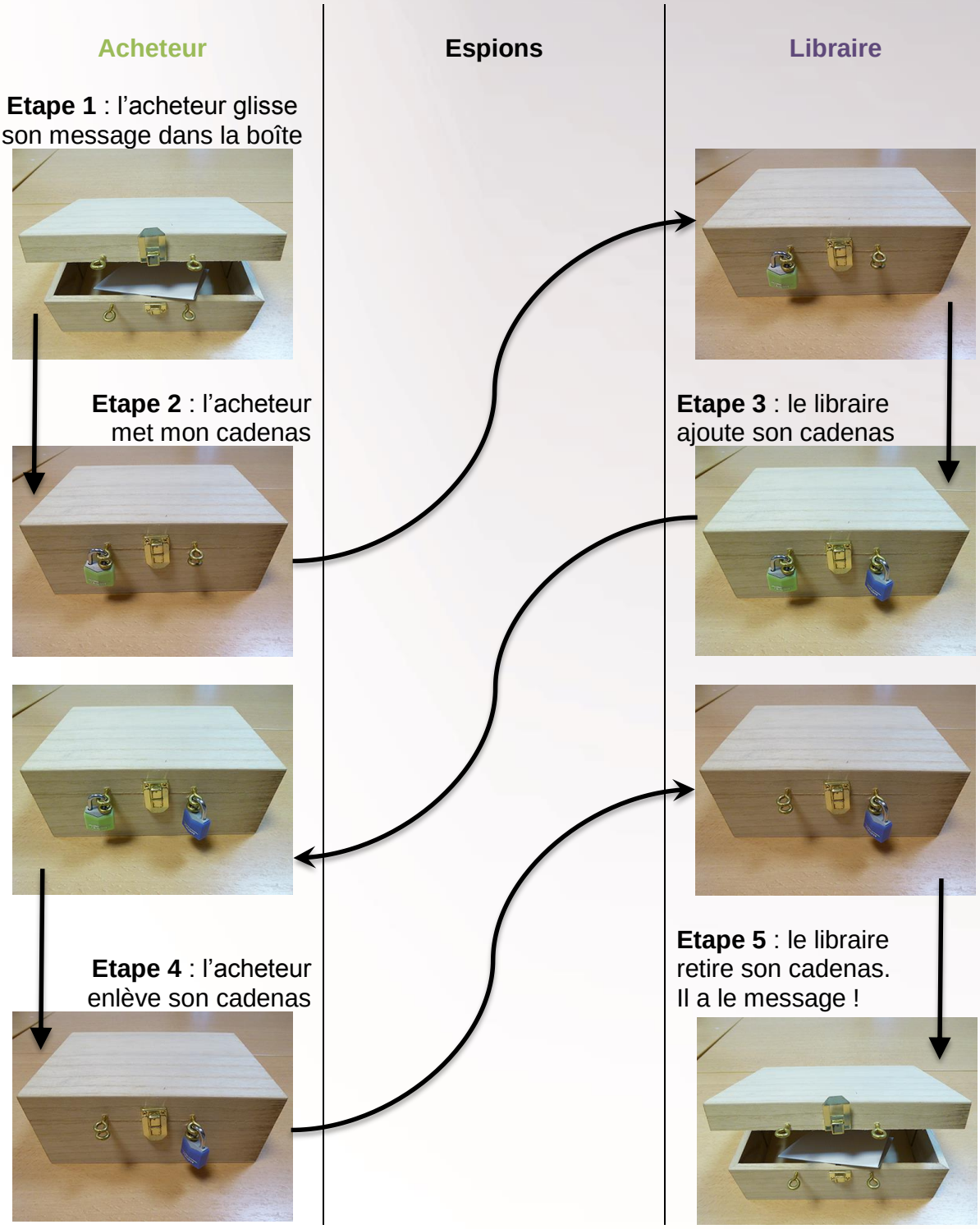
Le groupe « acheteur » veut envoyer le code de la carte bleue au libraire. Les acheteurs ont une boite à deux serrures où ils pourront glisser leur message, c'est-à-dire le code. Le groupe « acheteur » et le groupe « libraire » ont chacun un cadenas, avec une clé. Ils garderont toujours cette précieuse clé privée avec eux.

Quant aux espions, ils n'ont pas le droit d'aller dans le camp de l'acheteur ou du libraire, de voler la boite sur le parcours. Mais ils peuvent voler le cadenas s'il n'est pas attaché à la boite ou voler le message si la boite est ouverte !

Aux acheteurs et aux libraires de faire des essais jusqu'à ce que le message puisse passer.

Expérimentation

Comment l'acheteur envoie son code secret au libraire :



Selon la pédagogie et le niveau de participation des élèves on pourra soit leur faire construire eux-mêmes le jeu à partir du dessin de la page précédente soit mettre en œuvre une démarche d'investigation. Avec la règle « pas de cadenas ouvert hors du groupe ou du camp », les élèves recherchent alors une solution.

Pour réussir à faire passer le message, on le glisse dans une boite, avec un cadenas pour l'émetteur, et un pour le récepteur La boîte qui contient le message doit toujours avoir un cadenas quand elle va d'un ordinateur à l'autre et personne d'autre que le libraire ou l'acheteur ne peut l'ouvrir. Chacun garde précieusement la clé du cadenas et les cadenas restent toujours fermés lors du transport, pour que personne ne puisse voler son contenu.

Nous utilisons tout le temps ce système pour faire communiquer les ordinateurs entre eux. On rappelle bien que ce ne sont pas des vraies boites et de vrais cadenas, c'est juste une façon d'expliquer ce qui se passe dans les ordinateurs.

Conclusion

Dans le monde numérique, ce qui tient lieu de « cadenas », c'est un calcul qui va prendre le message initial et le mélanger avec une formule mathématique pour en faire un message crypté. De ce calcul, seul l'émetteur du message a la clé (c'est-à-dire le code pour réaliser le calcul à l'envers afin de retrouver le message initial).
Ici on voit que chacun applique son calcul de mélange, puis de démêlage. On note aussi que, pour que ça marche, il faut pouvoir intervertir les deux calculs puisque le démêlage par l'émetteur se fait sur le message mélangé par le récepteur.

On pourra aussi expliquer que le cadenas est une « clé publique » tandis que la clé du cadenas (ou la combinaison du cadenas) est la « clé privée ».

On retiendra que c'est un américain appelé Whitfield Diffie qui a inventé ce type de système de code secret de systèmes numériques.

Sources :

CNRS – Images des mathématiques
http://images.math.cnrs.fr/Dis-maman-ou-papa-comment-on-cache.html
Pixees, ressources pour les sciences du numérique
https://pixees.fr/?p=741

POUR ALLER PLUS LOIN

L'aventure des Sépas, web-série de 20 dessins animés en 3D où les terriens apprennent la science aux extra-terrestres.
Vidéo « Les Sépas et la cryptologie » :
https://files.inria.fr/mecsci/grains-videos3.0/videos/19-cryptologie.mp4