Sujet ? **Cryptographie et protection des données**

Degré ? Cycle 2 (5-6H)

Objectifs ?

S'approprier les concepts de base de la science informatique…

2…en encodant, en cryptant et en transformant des données informatiques

Information et données

- Cryptage et décryptage d'un message à l'aide de méthodes simples.

Capacités transversales ?

- **Collaboration** (échanger des points de vue ; participer à l'élaboration d'une décision commune et à son choix)

- **Pensée créatrice** (varier ses sources d'inspiration ;faire le choix de stratégies et de techniques inventives ; expérimenter des associations inhabituelles ; accepter le risque et l'inconnu)

Modalités de mise en oeuvre ?

- La classe est composée de 20 élèves.

- Ils sont répartis en 4 îlots de 5 élèves.

- Choix de la méthode de travail : par groupe (par vague) :

La séquence est divisée en séances. Chaque séance travaille un concept de la cryptographie (confusion, diffusion). Ces séances sont divisées par niveaux (progressifs). Dès qu'un groupe termine un niveau, il passe au suivant. Cela permet de différencier les différents niveaux et la vitesse variable des différents groupes.

Pour ce faire, il y a 5 niveaux par sujet (3 minimum dont 2 bonus). A la suite des deux niveaux bonus, les élèves peuvent faire une activité branchée sur les ipads/ordinateurs (mastermind) en lien avec la cryptographie.

À la fin de chaque cours, il y a un moment d'institutionnalisation (fait avec et par les élèves) afin de clarifier la matière et les éléments à retenir. Ce moment peut prendre différentes formes :

- Discussion orale avec questions ouverte : « Qu'avez-vous appris durant ce cours sur la cryptographie ? »
- Jeu de la balle : je pose une question fermée « Qu'est-ce que la cryptographie, à quoi sert la cryptographie, quel principe de cryptographie avons-nous étudié aujourd'hui, quels sont les différentes méthodes/techniques pour faire de la diffusion, etc. » et je lance la balle aux élèves qui lèvent la main pour répondre.
- Synthèse écrite individuelle => mise en commun.

Matériel ?

- 4 ordinateurs + 3 ipads.
- 5 Fiches d'introduction
- 5 Fiches pour le principe de confusion (5 niveaux)
- 5 Fiches pour le principe de diffusion (5 niveaux)
- Fiche pour le jeu du trésor (informaticiens et hackers).
- Fiche d'institutionnalisation finale .

Déroulement général ?

1. Activités d'introduction (1 cours)

- Quel est le thème ?
- Test diagnostique
- A quoi sert la cryptographie ?
- Institutionnalisation

2. Une séance sur le principe de confusion (1 cours)

- Rappel du connu.
- 5 niveaux correspondants à 5 exemples de confusion différents (3 minimum et 2 bonus).
- Activité branchée (mastermind).
- Institutionnalisation.

3. Une séance sur le principe de diffusion (1 cours)

- Rappel du connu.
- 5 niveaux correspondants à 5 exemples de confusion différents (3 minimum et 2 bonus)
- Activité branchée (mastermind).
- Institutionnalisation.

4. Mise en pratique : les hackers et les informaticiens : envoi d'un message crypté. (1 cours)

- Rappel du connu.
- Jeu du trésor : 3 groupes (ceux qui transmette le message et la clé, les informaticiens et les hackers qui doivent décrypter la clé puis le message afin de connaître le lieu du trésor = premier arrivé = gagnant.
- Mastermind en branché (pendant l'attente des différents groupes)
- Institutionnalisation.

En détail ?

Cours 1 : Activités d'introduction

1. Quel est le thème ?	- Entrée en classe. - L'enseignant distribue des images à chaque îlot (une clé, password etc.). - Les élèves doivent trouver par groupe le point commun entre les différentes .images = la thématique. - Mise en commun.	Par groupe	10'
2. Test diagnostique	- L'enseignant dit le contexte : nous allons inventer un mot de passe oral pour rentrer en classe. Il faut crypter le mot bonjour.	Individuel	20'
3. À quoi sert la cryptographie ?	- L'enseignant distribue des 3 pages à chaque îlots (chaque page contient une utilité spécifique de la cryptogrpahie). - Les élèves doivent trouver par groupe le point commun entre les différentes images = une utilité . - Mise en commun.	Par gropue	10'
4. Institutionnalisation avec jeu	- Jeu de la balle : je pose une question fermée « Qu'est-ce que la cryptographie, à quoi sert la cryptographie, etc… » et je lance la balle aux élèves qui lèvent la main pour répondre.	Collectif	5'

Cours 2 : Une séance sur le principe de confusion

1. Rappel du connu	- Entrée en classe. - Au tableau noir. Mind map fait au collectif avec au centre (la cryptographie). Deux mots écrits par l'enseignant (Quoi et utilité) Posez les questions suivantes si besoin de guidance : Qu'avons-nous fait la dernière fois ? Qu'est-ce que la cryptographie ? À quoi cela sert-il ?	Coll.	5'
2. 5 niveaux progressifs (= 5 exemples de techniques de cryptographie utilisant le principe de confusion comme par exemple la méthode César	- Les élèves travaillent par groupe (=îlot). - Chaque groupe reçoit la première fiche (= première technique de confusion). - Travail en 2 étapes : A) Réception : Analyser les 3 exemples cryptés avec version décryptée afin de trouver et noter la technique utilisée (grâce à la théorie de la variation de Marton) B) Production : essai de cryptage d'un message simple avec cette technique. - Une fois le niveau 1 terminé (fiche 1), le groupe passe au niveau 2 et ainsi de suite. - Les niveaux sont de plus en plus difficiles. Soit par la technique utilisée soit par la réduction des aides. Par exemple les deux niveaux bonus n'ont pas d'exemples crypté=>décrypté. Le but est de trouver la technique seul (défi !) - Misse en commun des travaux : débat socio-cognitif, maintien de l'incertitude afin de laisser les élèves débattre et justifier leurs réponses.	Par groupe Coll.	35'
3. Activité supplémentaire branchée (mastermind)	- Si le temps (5 niveaux terminés) - Application : Guess the code pro (Mastermind) sur mac et/ou Ipad.	À 3 par machine	
4. Institutionnalisation orale	- Discussion orale avec questions ouverte : « Qu'avez-vous appris durant ce cours sur la cryptographie ? » - Si rien d'essentiel ne sort, ciblez sur des questions fermées du type : « Quelle principe de cryptographie avez-vous découvert et utilisé aujourd'hui ? Pouvez-vous nous donner des exemples de différentes techniques utilisant ce principe ?	Coll.	5'

Cours 3 : Une séance sur le principe de la diffusion

4. Rappel du connu	- Entrée en classe. - Au tableau noir. Mind map fait au collectif avec au centre (la cryptographie). Principe de confusion écrit en grand. Posez les questions suivantes si besoin de guidance : Qu'avons-nous fait la dernière fois ? Qu'est-ce que lle principe de confusion en cryptographie ? À quoi cela sert-il ? etc.	Coll.	5'
5. 5 niveaux progressifs (= 5 exemples de techniques de cryptographie utilisant le principe de la diffusion comme par exemple le langage javanais.	- Les élèves travaillent par groupe (=îlot). - Chaque groupe reçoit la première fiche (= première technique de diffusion). - Travail en 2 étapes : C) Réception : Analyser les 3 exemples cryptés avec version décryptée afin de trouver et noter la technique utilisée (grâce à la théorie de la variation de Marton) D) Production : essai de cryptage d'un message simple avec cette technique. - Une fois le niveau 1 terminé (fiche 1), le groupe passe au niveau 2 et ainsi de suite. - Les niveaux sont de plus en plus difficiles. Soit par la technique utilisée soit par la réduction des aides. Par exemple les deux niveaux bonus n'ont pas d'exemples crypté=>décrypté. Le but est de trouver la technique seul (défi !) - Misse en commun des travaux : débat socio-cognitif, maintien de l'incertitude afin de laisser les élèves débattre et justifier leurs réponses.	Par groupe Coll.	35'
6. Activité supplémentaire branchée (mastermind)	- Si le temps (5 niveaux terminés) - Application : Guess the code pro (Mastermind) sur mac et/ou Ipad.	Ind.	
4. Institutionnalisation orale	- Discussion orale avec questions ouverte : « Qu'avez-vous appris durant ce cours sur la cryptographie ? » - Si rien d'essentiel ne sort, ciblez sur des questions fermées du type : « Quelle principe de cryptographie avez-vous découvert et utilisé aujourd'hui ? Pouvez-vous nous donner des exemples de différentes techniques utilisant ce principe ?	Coll.	5'

5. Cours 2 : Mise en pratique : les hackers et les informaticiens : envoi d'un message crypté. (1 cours)

1. Rappel du connu	- Entrée en classe. - Au tableau noir. Mind map fait au collectif avec au centre (la cryptographie). Deux mots écrits par l'enseignant : principe de confusion et de diffusion. <u>Posez les questions suivantes si besoin de guidance :</u> Qu'avons-nous fait la dernière fois ? Qu'est-ce que la cryptographie ? À quoi cela sert-il ? Quels sont les deux principes/techniques de cryptographie ? Donner moi des exemples, etc.	Coll.	8'
2. Jeu du trésor : des informaticiens et des hackers	- Les élèves sont répartis en 3 groupes (ceux qui font le message, les informaticiens et les hackers qui doivent décrypter en premier ce message). - Le groupe 1 (ceux qui font le message) choisissent un message simple correspondant à un objet/meuble présent dans la salle de classe (le premier groupe (hacker ou informaticiens) qui le décryptera devra se rendre vers cet objet/meublier afin de trouver un trésor) - Le groupe 1 choisisse une clé qui servira à crypter et décrypter le message. Ils écrivent cette clé avec le principe de la diffusion (version simple) sur un message secret qui sera transmis au informaticien et vu/volé par les hackers. => transmission - Pendant le temps que les hackers et les informaticiens cherche à trouver la clé, le groupe 1 crypte leur message. => transmission - Les hackers et les informaticiens s'affrontent dans une course de vitesse afin de trouver la clé, décrypter le message et de se rendre vers le trésor.	Par groupe Coll.	30'
3. Activité d'attente branchée (master mind)	- Pendant que le groupe 1 travaille au début : les hackers et les informaticiens peuvent jouer. - Une fois que le groupe 1 a terminé sa double transmission (clé et message), les élèves peuvent aller jouer. - Application : Guess the code pro (Mastermind) sur mac et/ou Ipad.	Ind.	
4. Institutionnalisation écrite	- Synthèse écrite individuelle : à partir de la question : « Qu'avez-vous appris la cryptographie ? Que savez-vous faire ? Donnez des exemples » - Mise en commun.	Ind. Coll.	8'