Nahuel Degonda nahuel.degonda@edu-vd.ch

Planning du cours :

Temps	Dénomination et support	Déroulement	Mode de travail
5min	Accueil PowerPoint	Prévenir qu'une élève fera son test, demander le respect de celle-ci. Indiquer que le cours d'aujourd'hui est sans ordinateur, la semaine prochaine iels auront leurs notes du test et qu'on commencera le stop-motion	Collectif
10min	Introduction exercice message codé sur papier Papier, stylos PPT	Activité sans donner de contexte : « Si je voulais faire parvenir un petit mot à un·e camarade de classe et que je ne voulais pas que le prof (moi) le comprenne, comment faire ? » Les élèves doivent, par groupes de 3, inventer une technique pour écrire un message sur papier et faire en sorte que je ne le comprenne pas si je venais à le lire. Laisser les élèves inventer leurs messages. Proposer des idées de messages au tableau pour les moins inspiré·e·s (Où on se retrouve et à quelle heure samedi, On va manger quoi à midi, Qui va gagner la coupe du monde de [sport] ?) La consigne demande De proposer une solution en écrivant un exemple, les groupes ayant rapidement fini peuvent chercher d'autres solutions. Mise en commun au tableau (ou sur le PowerPoint si salle adaptée à la manipulation devant les élèves) : demander aux élèves de montrer/lire leur exemple, jouer le jeu et voir si je peux comprendre le message, demander aux autres élèves s'iels y arrivent. Utiliser la slide 3 du PowerPoint pour décomposer les méthodes et la slide 4 pour mettre les premiers termes techniques sur les concepts abordés.	Petits groupes (3) puis collectif

Nahuel Degonda nahuel.degonda@edu-vd.ch

10min	Présentation du plan du cours et explication du sens de cette leçon en cours d'informatique PPT	Slides 5 et 6 du PPT Expliquer ce qu'est la cryptanalyse, le décryptage, et les méthodes de cryptage. Comment historiquement on avait besoin de crypter des messages (données) et comment aujourd'hui ça nous impacte. Interroger les élèves s'iels ont des exemples (mots de passe, comment ils sont stockés, etc…) Introduire le défi de « Et vous ? Pourriez-vous casser le code de Jules César ? »	Collectif
20min	Activité cryptage substitution Fiche 1 +PPT	Fiche 1 par les élèves en binôme (voire groupes de 3) Donner Fiche 2 aux groupes plus lents/en difficulté Mise en commun des techniques des élèves, expliquer comment les décrypter (Slide 7)	Binômes (ou 3) puis Collectif
20min	Activité Chiffrement de César (élèves) Fiche 3, 3bis, 4 et 5 PPT	Slide 8, les élèves tentent de décrypter les textes plus complexes (Fiche 5) en leur donnant des outils (Fiche 3, 3bis et 4) (sans leur expliquer, trial and error), aider les bloqué·e·s. Les groupes ayant compris rapidement peuvent faire la fiche 5 Afficher les slides 9 puis 10 au fur et à mesure si trop de groupes demandent de l'aide.	Binômes (ou 3)
10min	Mise en commun chiffrement de César	Mise en commun à l'aide des slides 11 et 12 : Parler des méthodes que les élèves ont utilisées, fréquence des lettres ? Déduction ? Utilser les outils de déchiffrage ?	Collectif

Nahuel Degonda nahuel.degonda@edu-vd.ch

	Fiche 5 PPT	Demander à des élèves de montrer leur méthode, utiliser le PPT à l'appui pour montrer aux élèves plus éloigné·e·s) Expliciter le chiffrement de César à l'aide des slides 13 et 14, si le temps ne permet pas de faire le chiffrement mono-alphabétique, laisser les élèves faire la fiche 5 en entier.	
10min	Activité chiffrement mono-alphabétique Fiche 6 PPT	Expliquer la méthode de chiffrement mono-alphabétique à l'aide de la slide 15, de sa nécessité à cause des limites de 25 variétés de méthodes de substitution César. Les laisser faire la Fiche 6. Corrections communes	Binômes (ou 3) puis collectif
Fin	Conclusion	Institutionnalisation des savoirs : slides 16 et 17 pour rappeler les divers concepts clés aujourd'hui, ce qu'il y a à retenir, leur rappeler leur réussite (potentielle) d'avoir été « plus malin » que Jules César. Ranger et récupérer le matériel (si réutilisable et/ou si les élèves n'expriment pas l'envie des les garder. Si des cylindres de décodage ont été imprimés en 3D, probablement qu'iels voudront les garder)	Collectif

Nahuel Degonda nahuel.degonda@edu-vd.ch

Références

- Cryptographie Débranchée https://fondation-lamap.org/sequence-d-activites/cryptographie-debranchee
- Outil pour cryptanalyse par fréquence https://jp.pellet.name/hep/decrypt/?n=0&type=freq
- Lien vers support de présentation PowerPoint Cryptographie.pptx
- Lien vers fiches d'exercices et outils à découper Fiches et outils cryptage.pdf