Utiliser le hachage pour vérifier l'intégrité

Code de l'activité Capytale : 7f07-3436308

Remarque générale :

- Les élèves doivent répondre en utilisant les cellules en texte. Le professeur peut changer le type de cellule pour utiliser le markdown (cycle 4 technologie, classe de SNT en langage balisé).
- On pourra trouver l'écriture anglaise hashage au lieu de hachage.

Déroulé de la séquence :

Séance 1 : mathématiques (collège 3ème), SNT, NSI.

- Visionnage de la vidéo, rendre le questionnaire avant la séance (**Devoir maison**). A la question qu'est ce que l'intégrité, l'utilisation d'une IA par les élèves va permettre de tester l'esprit critique des élèves par rapport aux propositions d'une IA générative.
- **Début de séance** : bilan du questionnaire, puis présentation de MITM. Explication de l'attaque passive où l'attaquant espionne sans modifier. Présentation de l'attaque active où l'attaquant se fait passer à la fois pour Bob et pour Alice avec modifications des messages.
- Intérêt de la double authentification. Faire le lien avec Pix et la sécurisation. Compétences du CRCN :

  Domaine 4 : Protection et sécurité
  - Compétence 4.1 Sécuriser l'environnement numérique
  - Compétence 4.2 Protéger les données personnelles et la vie privée

  L'attaque de l'homme du milieu est au programme de la classe de Terminale, mais la connaissance du terme fait partie de la culture informatique.
- **Activté débranchée :** utilisation du tableau de correspondance lettre majuscule et position dans l'alphabet. Les élèves doivent chercher des anagrammes de 4 lettres puis calculent à la « main » l'empreinte naïve. Ils testent ensuite leurs résultats à l'aide de la fonction empreinte_naive qui a été implémentée dans le notebook. Il y a collision d'où l'intérêt de créer une fonction empreinte plus complexe.
  Le code de la fonction est donnée. Ils utilisent la méthodologie PRIMM pour celle-ci.

La méthodologie PRIMM , développée par Sue Sentance, est une approche structurée pour enseigner la programmation en cinq étapes :

- **Prédire** le comportement d'un programme ;
- **Exécuter** le code pour vérifier ;
- **Investiguer** son fonctionnement ;
- **Modifier** des parties existantes ;
- **Créer** de nouveaux programmes.

Conçue pour réduire la charge cognitive des débutants, elle insiste sur la compréhension du code avant l'écriture, en intégrant des discussions et des activités collaboratives.

Challenge tous niveaux : on prend un mot, trouvez un autre mot ayant le même condensat. Ecrire un programme permettant de trouver ce mot.

Timing : 30'

- **Partie 2 : modification avec texte.**

Expliquer prolongement pour expliquer l'effet cascade.

Maison : donner la table ASCII pour calculer une empreinte de mot de 5 lettres. Explication de ce qu'est l'ASCII.

Timing : 55'

Séance 2 : NSI

Points du programme en NSI :

- Sécurisation : attaque de l'homme du milieu (Terminale);
- Utilisation de bibliothèques ;
- Algorithmique : structures de données, boucles…
- Histoire de l'informatique : Turing (Première & Terminale)

Points du programme SNT :

- Photographie numérique
- Algorithmes

Compétences du CRCN :

Domaine 4 : Protection et sécurité

- Compétence 4.1 Sécuriser l'environnement numérique
- Compétence 4.2 Protéger les données personnelles et la vie privée

Introduction :

Une image est un tableau de nombre, puis explications du passage en niveau de gris.

Activité obtention de ce tableau. Conversion en niveau de gris.

En vous inspirant de la fonction empreinte de la séance 1, écrire la fonction empreinte_image permettant de calculer le hash d'une image en niveau de gris.

Maison : recherche sur Alan Turing. Ouverture Grand oral

Pour aller plus loin : des idées de grand oral : différentes attaques possibles, les personnages clés de l'informatique Turing Church…

Annexes

Liste des anagrammes de 4 lettres en Français, à adapter en majuscule :

4 lettres	
mari	mira rima rami
main	mina
fois	soif
état	téta
peur	pure
face	café
ange	nage
rame	mare
sure	ruse
vrai	vira
avec	cave
mien	mine
rose	oser