

Présentation de l'activité

L'activité se décompose en deux parties :

Partie1 : des éléments concernant le hachage sont donnés. Mise en situation : Les élèves découvrent ensuite une fonction de hachage simplifiée et l'intérêt de vérifier l'intégrité
Partie 2 : Production d'un programme permettant d'obtenir la signature d'un message ou d'une image

...

Public

Seconde SNT/ Première NSI

Objectifs



Savoirs SNT

Notions transversales de programmation

Connaissances

Écrire et développer des programmes pour répondre à des problèmes et modéliser des phénomènes physiques, économiques et sociaux

Compétences associées

- faire preuve d'autonomie, d'initiative et de créativité ;
- présenter un problème ou sa solution, développer une argumentation dans le cadre d'un débat ;
- coopérer au sein d'une équipe ;
- rechercher de l'information, apprendre à utiliser des sources de qualité, partager des ressources ;
- faire un usage responsable et critique des sciences et technologies numériques.

Savoirs NSI

Code ASCII, parcours séquentiels

Connaissances

-Parcours séquentiel d'un tableau

- Lire et modifier les éléments d'un tableau grâce à leurs index. Utiliser des tableaux de tableaux pour représenter des matrices : notation $a[i][j]$. Itérer sur les éléments d'un tableau.

Compétences NSI

- analyser et modéliser un problème en termes de flux et de traitement d'informations ;
- concevoir des solutions algorithmiques ;
- mobiliser les concepts et les technologies utiles pour assurer les fonctions d'acquisition, de mémorisation, de traitement et de diffusion des informations ;



Compétences numériques - cadre du CRCN

Domaine « Information et données » : compétence 3 « Traiter des données »

Niveau 5 : « Automatiser un traitement de données »

Domaine « Protection et sécurité » : compétence 2 « protéger les données personnelles et la vie privée. »

Niveau 4 : « Mettre en œuvre des stratégies de protection de sa vie privée et de ses données personnelles et respecter celles des autres »

Prérequis

Base de l'algorithmique

Déroulement de l'activité envisagé

Découvrir un moyen de vérifier l'intégrité d'un message ou d'une image.

Niveau SNT : Dans un premier temps, les élèves seront initiés à la notion de fonction de hachage à travers un exemple simplifié utilisant le codage ASCII. Cette approche vise à vulgariser le concept de manière accessible. Le scénario pédagogique mettra en œuvre la technique de l'attaque de l'homme du milieu (man-in-the-middle attack) pour illustrer les enjeux de sécurité liés au hachage

Niveau NSI : un travail plus approfondi sera proposé en s'appuyant sur le codage ASCII et son implémentation informatique. L'objectif sera d'approfondir la compréhension des fonctions de hachage et de leur rôle dans la sécurisation des données. Dans un second temps, le concept sera étendu au domaine du traitement d'images numériques. Les élèves découvriront le calcul de condensats (hash) d'images, permettant de vérifier l'intégrité d'un fichier image et de détecter d'éventuelles modifications. Cette progression pédagogique, partant d'une vulgarisation accessible pour aborder progressivement des notions plus avancées, vise à développer chez les élèves une solide compréhension des enjeux de sécurité numérique liés au hachage, tout en les initiant aux techniques et outils informatiques associés.

Code Capytale : 7f07-3436308