Attaques par "canal auxiliaire"

Maude Pupin et Julien Narboux

13 février 2020

Résumé

Description d'une activité d'informatique débranchée sur le thème des attaques par « canal auxiliaire ». Cette activité a été préparée lors de l'École sur la médiation informatique de la SIF en Juin 2018. L'idée de l'activité a été proposée par Pascal Lafourcade avec la participation de David Cachera et Cécile Pierrot.

1 Matériel

— Le dessin d'un clavier numérique (voir dernière page).
— Éventuellement un objet pour indiquer qu'un code est faux (lampe rouge ou morceau de papier)
— Un ordinateur pour la dernière partie en branchée.

2 Déroulé de l'activité

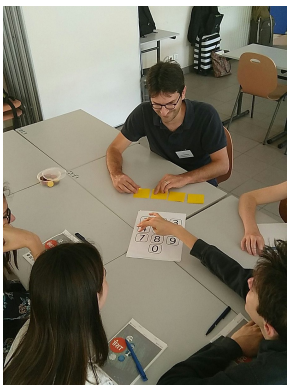
2.1 Introduction

On commence par la question : « Quelle est la différence entre un ordinateur et un humain ? » On attend la réponse : « ordinateur rapide mais bête, humain intelligent mais lent ».

« Bonjour, aujourd'hui vous allez ouvrir un coffre fort. Pour la première étape, je vais remplacer le coffre fort en exécutant un programme pour vérifier si le code est correct. Mais comme je suis un humain, je ne suis pas rapide alors allez lentement ! C'est une coffre fort mal conçu, vous allez donc peut-être pouvoir trouver la combinaison rapidement. Essayez ! »

2.2 Exploration du premier coffre

On choisit un code à quatre chiffres, on laisse les participants appuyer sur notre clavier en papier, **dès qu'un chiffre** est faux on l'indique à l'aide d'un objet ou en faisant un bruit [1].



D'expérience avec des élèves de secondes, les participants vont vite commencer à explorer plusieurs code et trouver la solution.

2.3 Analyse de l'exploration du premier coffre

Question : « Pourquoi ce coffre est mal conçu ? ». Réponse attendue : « Parce qu'il répond dès qu'un chiffre est faux sans attendre les quatre ».

On peut continuer en demandant combien d'essais au maximum il faudra réaliser pour trouver le code.

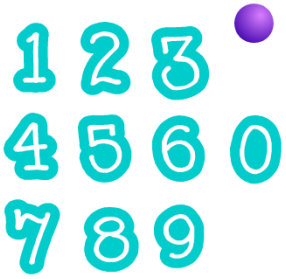
Réponse attendue : En 4*10 essais on sera sûr d'avoir trouvé le code.

À mettre en opposition avec le nombre de propositions à faire si on n'avait aucune indication pendant la saisie, ce qui correspond au nombre de codes différents à quatre chiffres. Il faut aussi leur demander combien il y en a. Pour aider on peut reformuler, « combien y a-t-il de possibilités pour le premier chiffre, etc. » Puis, s'ils ne trouvent toujours pas, on peut demander : « Jusqu'à quel nombre peut-on compter avec 4 chiffres ? »

1. La question se pose de savoir quel genre de digicode on simule, est-ce que l'on repart à zéro dès qu'un chiffre est faux ou est-ce qu'il faut un temps d'attente entre deux tentatives ?

2.4 Exploration du deuxième coffre

« Ok, c'était facile ! Maintenant, je vais vous proposer un deuxième coffre pas très bien conçu non plus. À vous de trouver la combinaison. »



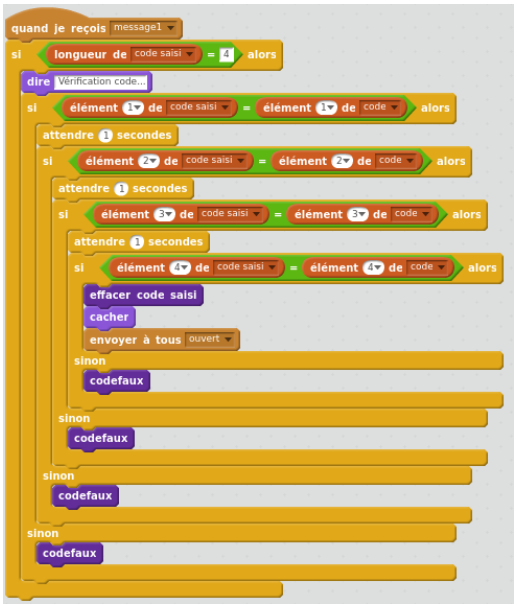
Ce coffre est matérialisé par un programme Scratch disponible ici.

On ne montre pas le programme aux participants, le coffre doit rester une boite noire. Le code secret est la date de naissance d'Ada Lovelace, ça permet éventuellement de faire une parenthèse en posant la question « Qui était le premier programmeur ? ».

Si les participants ne trouvent pas la faille, on peut donner une indication : « Est-ce que tu as un chronomètre sur toi ? »

2.5 Explications

« Ici notre exemple est simplifié pour que l'on puisse deviner le code en chronométrant grossièrement. Mais dans la réalité ce genre de failles ont déjà été exploitées : on peut exploiter par exemple le temps de réponse d'un algorithme qui décide si un code est correct ou non pour obtenir de l'information sur ce code. On peut aussi exploiter la consommation électrique, toutes les instructions exécutées par une carte à puce ne consomment pas forcement la même quantité d'énergie. Depuis que ce genre de failles est connu, on essaie de concevoir des puces qui consomment tout le temps la même quantité d'énergie. Pour plus d'informations voir l'article d'Hélène Le Bouder Des attaques informatiques utilisant la physique »



3 Retours d'expériences

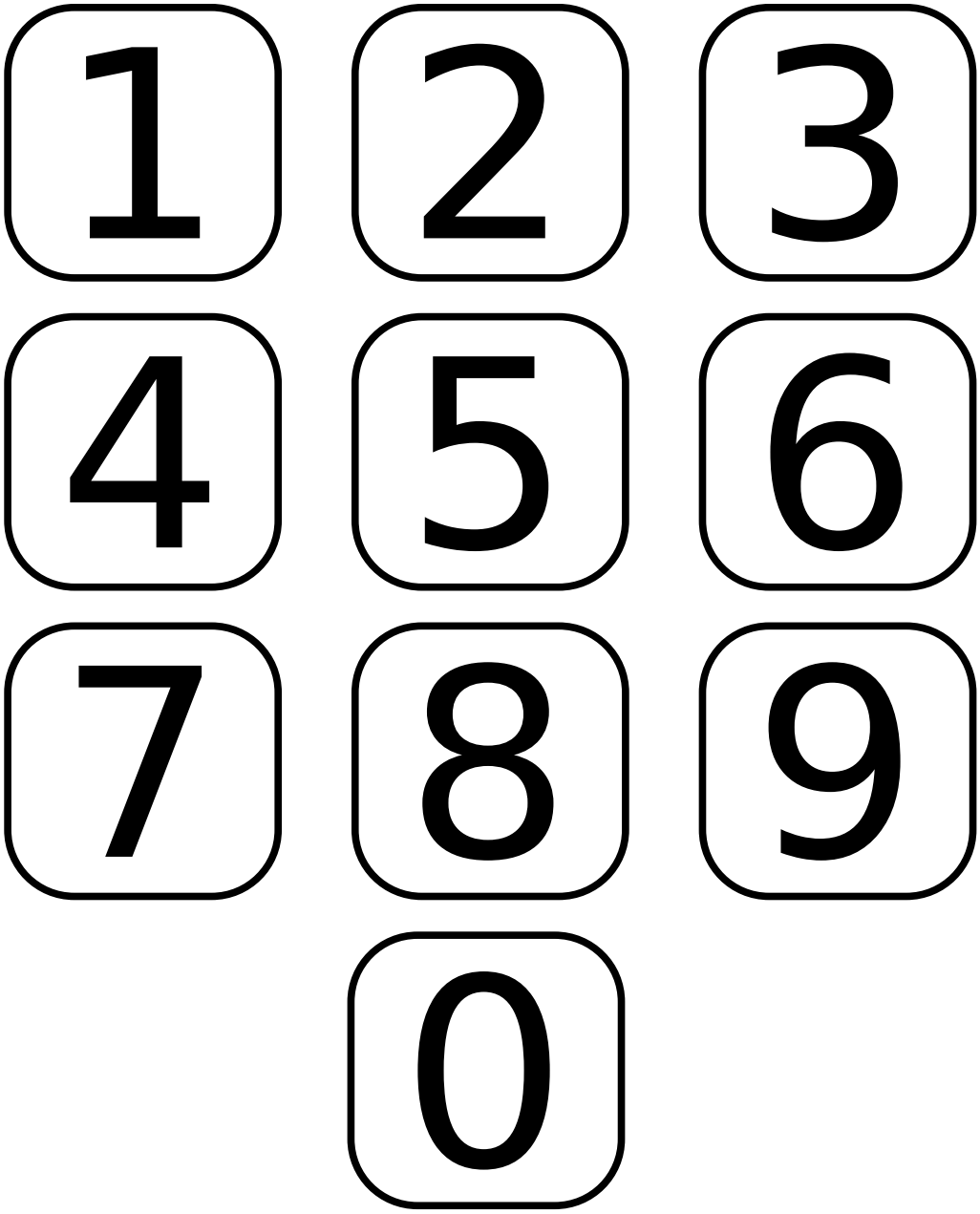
On a testé avec une classe de seconde uniquement en débranché, sans l'application Scratch. Il fallait environ 15 minutes pour faire l'activité (sans le deuxième coffre).

On pourrait améliorer l'activité en essayant de ne pas utiliser d'ordinateur. Voici deux pistes non explorées :

1. Remplacer le programme Scratch par un objet avec un vrai clavier et une LED pilotés par un Arduino.
2. Présenter l'activité sous forme d'un tour de magie :
   - Les participants choisissent un code à trois chiffres.
   - Quand le magicien essaie un code, ils doivent exécuter à la main un petit programme. Par exemple, le programme pourrait consister à dessiner des choses au moyens de feutres, le magicien ne voit pas les dessins mais uniquement les feutres utilisés, suivant les feutres utilisés on en déduirait le nombre de chiffres corrects.

4 Liens :

- Programme Scratch
- Wikipedia - Attaque par canal auxiliaire
- Article dans Interstices de Hélène Le Bouder


1
2
3
4
5
6
7
8
9
0