par P. Lafourcade et M. More

# L'attaque du digicode

**Dans cette activité, les élèves doivent utiliser astucieusement les indices fournis par un digicode d'un type un peu particulier pour découvrir efficacement le code permettant d'ouvrir une porte. Ce faisant, ils jouent le rôle d'un adversaire menant une attaque de sécurité.**

20 à 30 min. En binômes. À partir du cycle 4.
**Objectif :** Découvrir le concept d'attaque par canal auxiliaire.
**Compétences travaillées :** utiliser le dénombrement.

L'objectif de cette activité est de faire découvrir le concept d'*attaque par canal auxiliaire* (voir encadré) en imaginant un digicode dont les voyants lumineux laissent fuiter un peu d'information sur les chiffres du code d'entrée d'une porte. Le code comporte quatre chiffres, et le digicode possède dix touches portant les chiffres de 0 à 9 et deux voyants lumineux : un rouge et un vert. Quand un chiffre correct est saisi, le voyant vert s'allume, mais sitôt qu'un chiffre incorrect est tapé, le voyant vert s'éteint, le rouge s'allume et il faut recommencer à taper le code depuis le début.

Par exemple, si le code est 1234 et qu'Alice tape par inadvertance 124, les couleurs des voyants sont les suivantes :

1 → le voyant vert s'allume ;
2 → le voyant vert reste allumé ;
4 → le voyant vert s'éteint, le rouge s'allume et le code est annulé.

La question posée aux élèves est : quel est le nombre maximal d'essais qu'il faut effectuer pour ouvrir la porte sans connaître le code, pour une personne astucieuse ?

## Des informations auxiliaires à utiliser

Pour commencer, il est possible de mettre les élèves en activité en leur faisant jouer un jeu de rôle en binômes. Un élève choisit un code secret à quatre chiffres qu'il mémorise, pour jouer ensuite le rôle du digicode, pendant que son partenaire essaie de le deviner en indiquant les touches qu'il frappe sur le clavier. L'élève-digicode énonce seulement la couleur du voyant qui s'allume. Puis les deux rôles peuvent être permutés.

Pendant cette activité, les élèves trouvent rapidement les codes secrets : le nombre d'essais nécessaires est loin de 10 000, qui est le nombre total de codes différents composés de quatre chiffres de 0 à 9. Une fois qu'ils ont compris le fonctionnement des voyants vert et rouge, il est possible de leur demander de réfléchir à la méthode la plus efficace possible.

L'algorithme suivant apparaît rapidement : pour rechercher le premier chiffre du code, il suffit de tous les essayer un par un, jusqu'à ce que le voyant vert s'allume et ainsi être sûr de l'avoir trouvé. Cela prend au pire dix essais. Connaissant le premier chiffre, il est alors possible de rechercher le deuxième en tapant deux chiffres à la fois jusqu'à ce que le voyant vert s'allume de nouveau. En suivant cette stratégie, il suffit de dix autres essais au maximum. Ainsi, au total, en utilisant les voyants du digicode, il faut faire 10 + 10 + 10 + 10 = 40 essais dans le pire des cas pour ouvrir la porte.

Les élèves arrivent souvent à trouver cette stratégie et découvrent ainsi le principe des attaques par canal auxiliaire. En effet, les informations apportées par les couleurs des voyants laissent fuiter des informations permettant de retrouver en seulement quelques essais le code secret, au lieu des dix mille essais nécessaires dans le pire des cas en utilisant une méthode de recherche exhaustive (*brute force* en anglais).

Il est possible de faire encore un peu mieux ! En effet, si le voyant rouge s'allume encore au neuvième essai, alors il ne reste plus qu'une solution possible et il est inutile de faire le dernier essai. Le même raisonnement s'applique pour le deuxième et le troisième chiffres. En revanche, pour le dernier chiffre, si neuf essais au maximum suffisent toujours pour le découvrir, il faut bien ouvrir la porte, et donc taper le code une fois qu'il est découvert.
Finalement, 9 + 9 + 9 + 9 + 1 = 37 essais au maximum permettent d'ouvrir la porte.

## L'attaque par canal auxiliaire

En cryptographie, un *canal auxiliaire* (*side channel* en anglais) est un moyen détourné permettant d'obtenir des informations secrètes. Un exemple réel concerne les capteurs de température Netatmo qui indiquent, par défaut, publiquement sur Internet, la température observée là où ils sont placés. Il est donc possible de déterminer si une maison est habitée, simplement en observant ces valeurs.
Dans un cadre informatique, la mesure de la consommation électrique d'un processeur, ou celle du temps de calcul, peuvent permettre d'obtenir des informations sur les calculs effectués. Initialement, les attaques par canal auxiliaire ont été imaginées par Paul Kocher en 1996 lorsqu'il a montré qu'il était possible de découvrir les clés secrètes des chiffrements DES et RSA. Par exemple, dans la méthode RSA, le déchiffrement consiste essentiellement à effectuer un calcul d'élévation à une puissance, dans lequel l'exposant est la clé privée du destinataire. Comme les nombres en jeu sont « très grands » (plusieurs centaines de chiffres), un algorithme particulier, appelé l'*exponentiation rapide*, est utilisé pour aller vite. Cet algorithme effectue successivement des élévations au carré et des multiplications, en fonction des valeurs des bits de l'écriture en binaire de la clé privée. Comme l'élévation au carré est très légèrement plus rapide que la multiplication sur un processeur arithmétique, l'observation de la durée des opérations permet d'identifier leurs natures, et *in fine* de déduire l'ensemble des bits de la clé privée. Il est possible de se prémunir contre cette attaque en modifiant légèrement l'algorithme pour qu'il effectue des opérations inutiles afin de camoufler les différences de temps de calcul.

La conclusion des élèves après cette activité est souvent que les « vrais » digicodes ne fonctionnent heureusement pas comme celui qui leur est proposé ! Cependant, des attaques du même type existent réellement sur des systèmes informatiques.

**P. L. & M. M.**