

HORS-SÉRIE N° 103 : NOMBRES

L'énigme de la capsule temporelle est résolue !

Bernard Fabrot, un programmeur indépendant belge, est venu à bout d'une énigme posée il y a vingt ans par l'un des créateurs du système RSA. La solution n'était attendue qu'en 2035...

Les nombres sont au cœur de nombreuses énigmes, dont plusieurs étaient proposées dans le *Hors-Série* n° 103 : «L'ordre caché des nombres». L'une d'elles vient d'être résolue par le Belge Bernard Fabrot, programmeur indépendant.

En 1999, à l'occasion du 35^e anniversaire du Laboratoire d'informatique du MIT, le cryptologue américain Ronald Rivest (l'un des trois inventeurs de l'algorithme de cryptographie à clé publique RSA) enferme dans une «capsule temporelle» conçue par l'architecte Frank Gehry plusieurs objets offerts par les pionniers du numérique comme Bill Gates, Bob Metcalfe, Tim Berners-Lee... et promet le contenu à celui qui résoudra le défi suivant, noté LCS35 :

Calculer $w = 2^{2^t} \pmod n$, pour $t = 79685186856218$ et n un entier donné de 616 chiffres décimaux, produit de deux grands nombres premiers (qui ne sont pas connus). Trouver la valeur de w sans connaître la factorisation de n oblige à effectuer quelque 80000 milliards d'opérations itérées de mise au carré modul n en commençant par 2. À la fin, on peut traduire le résultat obtenu, w , en une phrase qui est le Sésame de la capsule.

Le problème a été conçu de façon à empêcher tout calcul parallèle. C'est un exemple de

«fonctions à retard vérifiable» (notées VDF pour *Verifiable Delay Functions*), aujourd'hui étudiées pour sécuriser les blockchains, sur lesquelles reposent, par exemple, le bitcoin ou Ethereum. C'est un des thèmes de recherche de Cryptophage, un groupe d'experts en cryptographie dirigé par Simon Peffers, d'Intel, qui planchait également sur le problème de Ronald Rivest. Ils ont été coiffés sur le fil par Bernard Fabrot.

Celui-ci a découvert par accident l'énigme en 2015. Il en est venu à bout à l'aide de GNUMP, une bibliothèque logicielle de calculs sur des nombres entiers, qui a accaparé une partie de son ordinateur personnel (plus précisément, un cœur du microprocesseur) 24 heures sur 24 et sept jours sur sept, vacances exceptées, pendant trois ans et demi. Il devance ainsi de quinze ans les prédictions de Ronald Rivest, fondées sur la loi de Moore.

Surprise, lorsqu'il envoie son résultat, le laboratoire de Ronald Rivest n'existe plus : il est intégré dans une entité plus grande (le CSAIL) dont la directrice n'a jamais entendu parler du problème. Tout s'est bien terminé, par une cérémonie le 15 mai 2019 lors de laquelle la capsule temporelle a été ouverte. ■

LE COMMUNIQUÉ DU CSAIL : [HTTP://BIT.LY/CSAIL-LCS35](http://bit.ly/CSAIL-LCS35)

Le contenu de la capsule temporelle est dévoilé devant notamment celui qui en a eu l'idée, Ronald Rivest (à droite), et celui qui a réussi à l'ouvrir, Bernard Fabrot (à sa droite).



Une mémoire fondée sur l'aléa

La mémoire de travail, l'une de celles décrites dans le *Hors-Série* n° 102 : «Les mutations de notre mémoire», permet notamment de garder à l'esprit le nécessaire à l'accomplissement d'une tâche. Comment fonctionne-t-elle ? Flora Bouchacourt et Timothy Buschman, de l'université de Princeton, aux États-Unis, proposent un nouveau modèle plus en accord avec les observations que les précédents, mettant en jeu des connexions aléatoires récurrentes selon deux «couches» neuronales, l'une étant liée aux perceptions sensorielles afin de maintenir l'afflux d'informations.

F. BOUCHACOURT
ET T. BUSCHMAN, *NEURON*,
PRÉPUBLICATION EN LIGNE, 2019

La nature, bonne pour... la nature

Les bains de nature sont bons pour la santé, les articles du *Hors-Série* n° 101 : «La révolution végétale» en attestent. Ils sont aussi bons pour la planète ! C'est le sens des résultats obtenus par Victor Cazalis (CEFE) et Anne-Caroline Prévot (CESCO). À partir de trois indicateurs (le score des candidats écologistes à diverses élections, le soutien aux associations environnementales et la participation à un programme de sciences participatives), ils ont montré que les Français ont des comportements d'autant plus écologiques qu'ils habitent dans un parc naturel (national ou régional), ou même simplement à proximité. On ne peut donc qu'encourager ces aires protégées, qui préservent le lien entre humains et nature, à poursuivre leurs actions. Et souhaiter voir le monde entier devenir parc naturel !

V. CAZALIS ET A.-C. PRÉVOT,
BIOLOGICAL CONSERVATION,
PRÉPUBLICATION EN LIGNE, 2019