Le Monde.fr

Retour sommaire

LES APPRENTIS DÉCODEURS

16/05/2016

David Larousserie

La relève en cryptographie est assurée. « Cent équipes de lycéens de 2de ont réussi à casser un code utilisé par les Allemands pendant la première guerre mondiale », souligne admiratif Razvan Barbulescu, chercheur au CNRS à l'Institut de mathématiques de Jussieu-Paris rive gauche. « Et trente sont venus à bout d'un code que nous avions nous-mêmes inventé, pensant que certains n'y arriveraient pas. Pour les départager, nous avons dû choisir les plus rapides. »

Trente-huit de ces brillants cryptanalystes amateurs, répartis en onze équipes, s'affronteront pour la finale de ce premier concours de cryptographie, baptisé Al Kindi, ce mercredi 18 mai au Musée de l'armée. Le lieu, tout comme l'un des partenaires, la Direction générale de la sécurité extérieure (DGSE), n'a évidemment pas été choisi au hasard tant la discipline a été utile aux militaires et aux espions. Aux côtés de la DGSE, Al Kindi est soutenu par l'éducation nationale et deux -associations de promotion – hors des laboratoires – des maths (Animath) et de l'informatique (France-IOI), à l'origine de l'initiative.

En décembre, 18 000 élèves, de toutes les académies, y compris de lycées français à l'étranger, se sont inscrits au premier tour de sélection. « C'est plus de 2 % des effectifs », se félicite M. Barbulescu, l'un des trois chercheurs, avec Matthieu Lequesne et Mathias Hiron, qui ont organisé ce concours « pendant plusieurs nuits ! ». Le nom fait référence à un mathématicien arabe du IXe siècle, dont les textes constituent la plus ancienne trace d'un travail de cryptanalyse consistant à compter les lettres et leurs fréquences pour décoder un message.

Cryptographie omniprésente

Cette première épreuve de décembre, toujours en ligne, consistait à relever différents défis : jeu sur les mots de passe, déchiffrement de textes obscurs, manipulation de machines à décoder… Trois niveaux, un système de points et un temps limité ont permis une première sélection. « On a souvent entendu des participants dire qu'ils prenaient plaisir à ces exercices. C'est la première fois qu'on l'entendait dans ce genre d'épreuves », témoigne Razvan Barbulescu, habitué à réaliser de tels concours.

La nature de la discipline explique sans doute ce succès. La cryptographie est omniprésente dans notre quotidien, avec les mots de passe pour accéder à des sites Web, les puces ou chiffres de cartes bancaires pour payer en ligne ou hors ligne, bon nombre de protocoles Internet authentifiant les sites ou garantissant la confidentialité des échanges, le vote électronique… « On n'a pas l'impression de faire des maths. Un message à déchiffrer est amusant en soi », constate aussi M. Barbulescu, qui donne cependant aussitôt des exemples de maths derrière ces applications : la factorisation des nombres entiers en nombres premiers, les opérations avec le logarithme, le recours à des courbes elliptiques.

(Suite page 5)

Retour sommaire

« Quinze filles en finale »

Pour les organisateurs, cette première série d'épreuves devait sensibiliser à la sécurité informatique et lutter contre quelques clichés. Pari réussi : « Quinze filles sont en finale, et il y a même une équipe uniquement féminine. Dans les sélections, tous les types d'élèves ont pris du plaisir », indique Matthieu Lequesne, étudiant à Polytechnique. « Même s'ils n'apprenaient rien en crypto, ils apprenaient au moins le travail d'équipe », ajoute-t-il.

Les trois épreuves suivantes, avant la finale, étaient plus « classiques » : déchiffrer un texte, codé notamment par des méthodes réellement utilisées pendant les guerres.

La finale, elle, durera une heure trente, sur papier et sans ordinateur. Il s'agira de décoder le plus de messages possible durant le temps imparti. Les premiers remporteront un ordinateur et une semaine de formation en informatique. Les meilleurs des différentes académies pourront visiter l'un des dix-sept laboratoires de cryptographie partenaires.

Les initiateurs ont bien l'intention de continuer avec un second concours, peut-être ouvert à de plus jeunes. Ils veulent aussi que le site Web se transforme en ressources pédagogiques et que davantage de chercheurs s'impliquent. « On voudrait aussi -trouver plus de problèmes parlant de cryptographie asymétrique, la grande invention du domaine, célébrée en 2015 par le prix Turing attribué à Diffie et Hellman », ajoute Matthieu Lequesne.