à la guerre moderne. Dorénavant, les savants serviront en tant que scientifiques, ou du moins dans les armes techniques, où ils seront moins exposés.

À la rentrée solennelle du 24 mars 1919, on commence à cultiver le souvenir de la Grande Guerre sur une double base : d'une part, le rappel du sacrifice de l'École et des promesses brisées que chaque vie perdue représente ; d'autre part, la réaffirmation de la mission de l'École en faveur de « la recherche libre et de la science désintéressée » et de la mission « pacifique et civilisatrice » de la France. Par contraste, l'École polytechnique représentera les ajustements qui doivent être apportés à ces idéaux à la suite de la guerre, notamment un investissement profond dans le développement de nouvelles applications des sciences pour l'industrie ou la guerre.

Dans les années 1920, les jeunes gens qui formeront plus tard Bourbaki sont abreuvés de ces discours. Quelques années plus tard, vers 1935, les membres du groupe entament la rédaction d'un nouveau traité de mathématiques très ambitieux, qu'ils veulent avant tout abstrait et défini par les seuls besoins internes aux mathématiques. Cette vision qu'ils promeuvent de plus en plus activement dans divers écrits à destination de larges publics jusque dans les années 1970 s'oppose de front à la conception promue par leurs aînés qui avaient plutôt tendance, comme on l'a vu, à penser les mathématiques dans la continuité des sciences de la nature.

Malgré cette opposition, ils entonnent volontiers le discours de leur *alma mater*. La mort de tant de mathématiciens pendant la guerre ne semble plus rien d'autre qu'un immense gâchis ; dorénavant, le but de la génération montante paraît clair : ils se doivent avant tout à la recherche mathématique pure. Les récits à propos des mathématiciens morts au combat, même si les membres de Bourbaki choisissent de ne pas s'en souvenir, ont rempli leur rôle : alors même que la recherche militaire est fortement promue par l'État, un large espace pour une science pure, neutre, s'est ouvert pour eux. C'est là, sans aucun doute, l'une des conséquences les plus durables de cette terrible guerre. ■

## BIBLIOGRAPHIE


**D. Aubin, L'Élite sous la mitraille**, Rue d'Ulm, 2018.

**D. Aubin et C. Goldstein (éd.), The War of Guns and Mathematics**, American Mathematical Society, 2014.

**P. Painlevé, L'École normale supérieure et la guerre**, *Revue scientifique*, vol. 54, p. 193-195, 1916.

**Notices nécrologiques de normaliens morts à la guerre :** https://www.presses.ens.fr/client/document/aubin_notices_834.pdf



RENDEZ-VOUS



# ENVOYER DES MESSAGES À RETARDEMENT

**La science cryptographique étudie les moyens de livrer une information en fixant une date avant laquelle elle restera cachée et inaccessible. Un problème de mieux en mieux résolu.**

**L'AUTEUR**

**JEAN-PAUL DELAHAYE**
professeur émérite à l'université de Lille et chercheur au laboratoire Cristal (Centre de recherche en informatique, signal et automatique de Lille)

Le 29 mai 1875, au milieu de la nuit, Frederick Deland, caissier à la Grand Mahawie Bank, est pris en otage par quatre individus qui se sont introduits chez lui. Conduit sur place à la banque, on lui demande d'ouvrir le coffre dont les malfrats savent qu'il connaît la combinaison. Il leur explique qu'un nouveau dispositif, empêchant d'ouvrir la porte du coffre avant une heure donnée, a été installé. Les menaces ne servent à rien et les voleurs repartent bredouilles.

Ce fut le premier succès des serrures à horlogerie, devenues alors d'usage courant et dont il existe une multitude de modèles différents, que les collectionneurs s'arrachent (*voir l'encadré 1*). Les banques en utilisent toujours, mais aujourd'hui vous en trouverez aussi pour les usages individuels sous le nom, en France, de serrures et coffres «à retardement». Il existe aussi des boîtes de rangement munies de tels dispositifs pour aider les victimes d'addiction à résister à leurs démons. On peut y déposer des téléphones portables, des paquets de cigarettes, de la drogue, de la nourriture, etc., qui, tant qu'ils sont dans la boîte fermée, empêchent qu'on y accède et en abuse.

## CAPSULES TEMPORELLES POUR LE MONDE NUMÉRIQUE

Et dans le monde numérique? Existe-t-il des «capsules temporelles» qui permettraient de chiffrer un message sous la forme d'un fichier informatique qu'on laisserait circuler, qu'on pourrait dupliquer et qui resterait illisible jusqu'à une certaine date, à partir de laquelle l'information cachée deviendrait accessible? La cryptographie moderne a abordé la question et les plus anciens travaux remontent à 1993. Le problème est assez délicat et les diverses solutions proposées ne réussissent que partiellement à créer ces capsules temporelles.

Pourtant de tels mécanismes de chiffrement à retardement seraient susceptibles de nombreuses applications. En voici quelques exemples.

– Vous voulez faire un cadeau à un proche pour son anniversaire. Vous lui envoyez un message chiffré qui se libère le jour venu et dans lequel est indiqué l'endroit où est caché son cadeau, ou les données pour accéder au compte où vous lui avez laissé une somme d'argent.

– Vous êtes un lanceur d'alerte… ou un maître chanteur. Vous déposez des informations compromettantes dans un endroit secret, peut-être sur internet, que vous ne voulez rendre publiques que si l'on vous arrête ou vous assassine. Vous faites circuler l'information sur le lieu du dépôt sous la forme d'un fichier temporairement chiffré jusqu'à une date que vous avez choisie. Si vous êtes arrêté ou tué, l'information sera libérée à la date choisie et tous ceux ayant reçu le fichier sauront, sans que vous ayez à intervenir, où sont les informations que vous vouliez rendre publiques.

– Pour organiser une enchère, chaque acheteur intéressé dépose le prix qu'il est prêt à payer dans un message chiffré qui ne se libère qu'à la date de clôture des enchères. Plus généralement l'idée fonctionne pour les procédures

Jean-Paul Delahaye a notamment publié : **Les Mathématiciens se plient au jeu**, une sélection de ses chroniques parues dans *Pour la Science* (Belin, 2017).