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

R
ENDEZ-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.

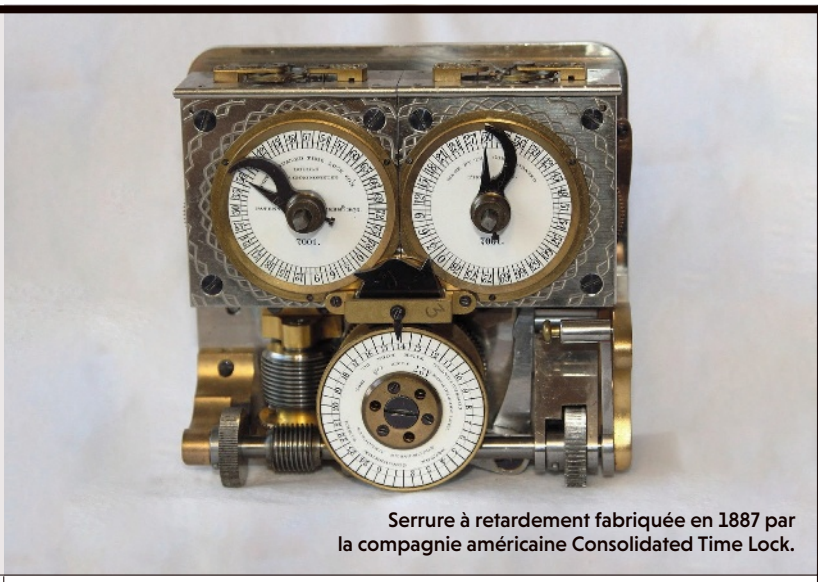
– Pour organiser une enchère, chaque acheteur intéressé dépose le prix qu'il est prêt à payer dans un message chiffré qui ne se libère qu'à la date de clôture des enchères. Plus généralement l'idée fonctionne pour les procédures

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

SERRURES À RETARDEMENT

1

Les serrures à retardement (*time lock boxes* en anglais), une fois enclenchées, ne peuvent pas s'ouvrir avant une heure programmée. Utilisées par les banques depuis plus d'un siècle, elles empêchent quiconque réussissant à entrer dans la salle des coffres, et même s'il connaît la combinaison d'un coffre, de l'ouvrir. Les modèles sont nombreux et intéressent les collectionneurs comme Mark Frank, qui a créé un magnifique site internet pour présenter sa collection, dont la photo ci-contre montre un exemplaire (www.my-time-machines.net/my_time_lock_collection.htm).



Serrure à retardement fabriquée en 1887 par la compagnie américaine Consolidated Time Lock.

de vote (non secret) où les électeurs sont éloignés et ne souhaitent dévoiler leur choix que lorsque chaque électeur a déposé le sien.

– Vous organisez un examen ou un concours dont les participants sont dispersés dans le monde entier. Sans avoir à vous soucier des délais et erreurs de transmission, vous leur envoyez la capsule temporelle contenant le sujet. Vous contrôlez que tous l'ont reçue et, à l'heure voulue, le sujet d'examen se dévoilera à tous.

COFFRES ET ORDINATEURS À RETARDEMENT

L'utilisation d'un coffre à retardement permet de maintenir secret un message jusqu'à la date programmée d'ouverture. Toutefois, le message n'est pas accessible à tout le monde à la date voulue. Un acteur puissant pourrait contrôler le coffre, l'ouvrir le premier et empêcher la diffusion de l'information déposée.

Pour éviter ce risque, vous pouvez mettre l'information dans plusieurs coffres en ne donnant l'information de leur emplacement qu'à certaines personnes. L'acteur puissant qui souhaite empêcher la diffusion de l'information ne connaîtra pas tous les emplacements des coffres.

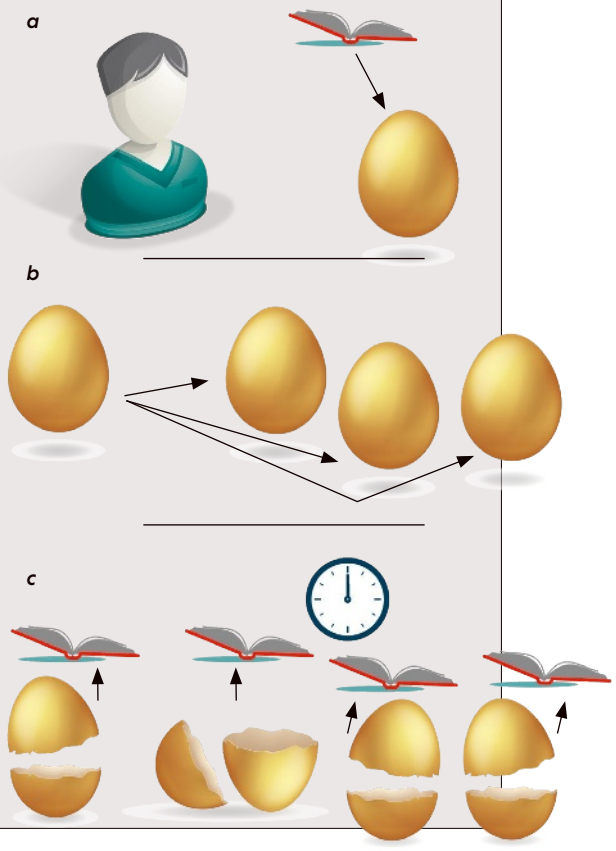
On peut aussi imaginer qu'avec une serrure à retardement, on envoie un message à une date donnée, par un téléphone portable où un ordinateur, à une série de numéros de téléphone donnés, ou, mieux, on dépose à une adresse internet le message souhaité qui sera alors lisible dans le monde entier. Un ordinateur portable caché dans un coffre fermé (qui laisse passer les ondes !) et convenablement >

2 UNE CAPSULE TEMPORELLE IDÉALE

Monsieur Dupont veut cacher l'histoire de sa vie qu'il a soigneusement rédigée et déposée dans un fichier informatique de façon à ce que personne de son vivant ne puisse en prendre connaissance. Il fixe la date de levée du secret au 1er janvier 2100. Il crée un fichier informatique (capsule temporelle) programmé pour cette date *(a)*.

Il fait ensuite circuler la capsule temporelle, qui est multipliée sur le réseau, sans que personne ne puisse prendre connaissance du contenu *(b)*.

Le 1er janvier 2100, ceux qui détiennent la capsule réussissent sans mal à l'ouvrir et à prendre connaissance du document de M. Dupont, qui est mort depuis longtemps *(c)*.



En haut : © Frank Mark (http://www.my-time-machines.net/)
En bas : © Shutterstock.com/Naida Jazmin Ochoa/Meilun/NeMaria/Pour la Science

3

UN SECRET PARTAGÉ EN MORCEAUX

Il est possible de partager un message M en n morceaux $M_1, M_2, \ldots, M_n$ de telle façon que l'on n'ait aucune information sur M tant que l'on ne dispose pas de tous les n morceaux. Expliquons comment. On suppose M donné sous forme binaire et ayant la longueur L.

Pour $M_1, M_2, \ldots, M_{n-1}$, on prend des suites de 0 et de 1 aléatoires, différentes et indépendantes, chacune de longueur L. Pour définir M_n, on procède bit par bit.

Pour le premier bit de M_n, on prend un 0 ou un 1 de façon que le nombre de 1 en première position dans les messages $M_1, M_2, \ldots, M_n$ soit pair si le premier bit de M est 0, et impair sinon.

Pour le deuxième bit de M_n, on procède de la même façon à partir des bits en deuxième position de M et de $M_1, M_2, \ldots, M_{n-1}$. Et ainsi de suite (la procédure est illustrée ci-dessous pour $n = 10$, sur un message court).

Connaître $M_1, M_2, \ldots, M_n$ permet de reconstituer M, mais connaître $n - 1$ de ces messages ne donne aucune information sur M.

On peut faire mieux et partager un message M en n morceaux de telle façon que :
– connaître k morceaux, quels qu'ils soient ($k < n$), redonne M ;
– connaître moins de k morceaux ne donne aucune information sur M.

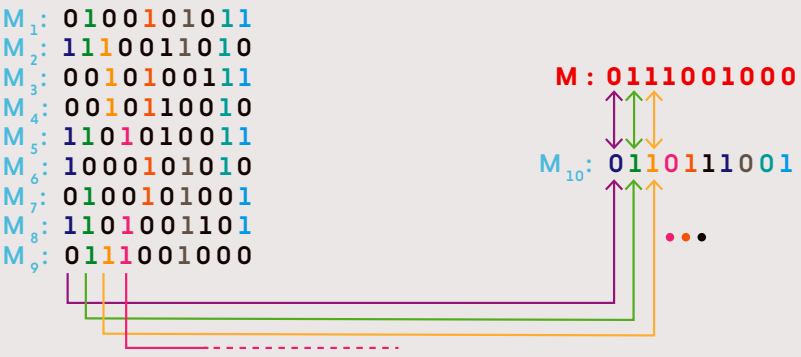
Plusieurs méthodes ont été proposées, dont celle d'Adi Shamir (« How to share a secret », *Communications of the ACM*, vol. 22(11), pp. 612-613, 1979).

Son idée repose sur le fait que disposer de k valeurs d'un polynôme P de degré $k - 1$ permet de le déterminer, mais que c'est impossible si l'on en connaît moins.

Le premier bit de M étant d_1, on commence par trouver un polynôme P_1 de degré $k - 1$ dont la valeur en 0 est d_1. Ensuite, pour chaque i de 1 à n, on fixe comme premier élément du message M_i la valeur $P_1(i)$.

On fait de même avec le second bit d_2 de M : on choisit un polynôme P_2 de degré $k - 1$ dont la valeur en 0 est d_2. Puis, pour chaque i de 1 à n, on fixe comme second élément du message M_i la valeur $P_2(i)$. Et ainsi de suite.

En conséquence :
– celui qui connaît k messages parmi $M_1, M_2, \ldots, M_n$ connaîtra le 1er bit de M, car il peut calculer le polynôme P_1. Il connaîtra le 2e bit de M, car il peut calculer le polynôme P_2. Etc.
– celui qui connaît moins de k messages parmi $M_1, M_2, \ldots, M_n$ ne peut rien connaître de M.



> programmé fera l'affaire : vous délivrerez le message à la date voulue.

Ces méthodes sont intéressantes, mais uniquement pour des délais assez courts ne dépassant pas quelques mois ou années, car les batteries du téléphone ou de l'ordinateur caché doivent tenir jusqu'au moment du déclenchement. Elles ne permettent pas d'envoyer un message un siècle à l'avance.

De plus, les solutions avec téléphone ou ordinateurs cachés ne produisent pas un fichier informatique qu'on laisse circuler et qui est tel que tous ceux le détenant à l'heure voulue en découvrent le message sans avoir à interagir avec autre chose. Elles ont aussi l'inconvénient d'être lourdes à mettre en œuvre, sans parler du risque que le dispositif caché soit découvert et arrêté ou détruit par accident. Réfléchissons à mieux.

FAIRE APPEL À UN OU PLUSIEURS TIERS DE CONFIANCE

Une idée évidente est celle du tiers de confiance. Vous confiez le message, placé dans une enveloppe cachetée par exemple, à un huissier en lui indiquant la date à laquelle il devra ouvrir l'enveloppe et en délivrer le contenu. Vous pouvez améliorer la robustesse du procédé en utilisant plusieurs tiers de confiance dont aucun ne pourra divulguer seul le message avant l'instant choisi par vous. Voici la méthode.

Vous découpez le message en n morceaux dont aucun ne permet d'avoir la moindre idée du message complet et dont même la connaissance de $n-1$ morceaux ne révèle rien (*voir l'encadré 3*). Vous confiez ces n morceaux à n tiers de confiance en leur demandant de se contacter les uns les autres à la date voulue pour s'échanger les bouts du message, le reconstituer et le rendre public.

Le risque sera cependant que l'un des tiers de confiance soit indisponible le jour voulu, malade ou décédé par exemple. Cela empêcherait que le message soit reconstitué et délivré. Mais il existe des procédés de découpage d'une information, inventés en 1979 par Adi Shamir et George Blakley, qui résolvent le problème. Le message est découpé en n morceaux qui ont la propriété que dès que l'on dispose de k morceaux ($k<n$) du découpage, il devient possible de retrouver tout le message, et qu'avec moins de k morceaux, rien ne peut être dévoilé du message découpé (*voir l'encadré 3*).

Ces idées résolvent sans doute un certain nombre de cas, mais, comme précédemment, ce ne sont que des méthodes partiellement satisfaisantes : elles ne produisent pas une capsule temporelle, c'est-à-dire un message qui libère seul son information à la date voulue à ceux qui le détiennent.

Explorons d'autres idées. Ronald Rivest