RENDEZ-VOUS

P.82 *Logique & calcul*
P.88 *Idées de physique*
P.92 *Chroniques de l'évolution*
P.96 *Science & gastronomie*
P.98 *À picorer*

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.

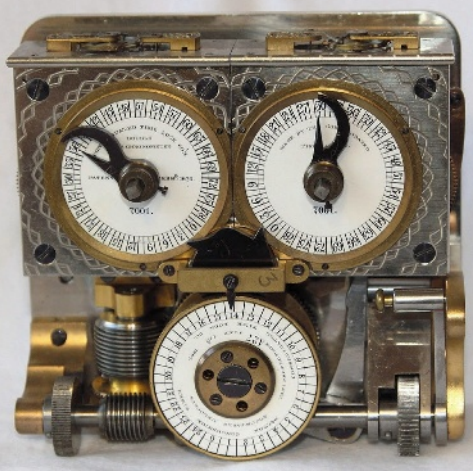
– Pour organiser une enchère, chaque acheteur intéressé dépose le prix qu'il est prêt à payer dans un message chiffré qui ne se libère qu'à la date de clôture des enchères. Plus généralement l'idée fonctionne pour les procédures

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)*.