> le 30 novembre 2019 à midi, qui donnerait un 0, donc *pile*; 3,5 °C pour le 1er décembre 2019 à midi, qui donnerait un 1, donc *face*; 5,2 °C pour le 2 décembre 2019 à midi, qui donnerait un 0, donc *pile*. La suite des tirages est donc, à partir du 28 novembre: *pile-face-pile-face-pile*. On peut opérer un tirage à pile ou face par téléphone tous les jours à midi.

Cette balise est très probablement aléatoire: il n'y a aucune raison de penser que les nombres pairs (ou impairs) soient favorisés, ni qu'aucune séquence particulière de *pile* ou *face* soit plus fréquente qu'une autre de même longueur. Elle est bien imprévisible, car les prévisions météorologiques pour Paris ne sont pas assez précises pour qu'on puisse savoir à l'avance ce qui va venir comme premier chiffre après la virgule de la température à midi. La balise est vérifiable *a posteriori*: tout le monde peut aller consulter le site mentionné pour voir ce qui y est indiqué. On peut raisonnablement faire confiance au sérieux des opérateurs du site pour qu'ils ne changent pas les données inscrites et qu'ils les maintiennent accessibles assez longtemps.

Trois problèmes persistent cependant avec cet aléa public.

(1) Prévoir le résultat du tirage devient possible quand on s'approche de midi, car la température varie continûment. Il faudrait donc convenir au moins quelques heures avant midi que l'on va jouer à pile ou face et attendre midi pour que s'effectue le tirage.

(2) Le procédé n'est pas rapide. En considérant d'autres lieux de relevé, d'autres heures, d'autres données (pression, hygrométrie, etc.) on pourrait faire mieux, mais on resterait limité à quelques bits par minute au plus.

(3) Peut-on faire totalement confiance à ce qui est publié par le site de Météo-France? Est-ce qu'il ne se pourrait pas qu'un employé, par négligence, erreur de manipulation ou soudoyé par l'un des joueurs, modifie le relevé publié pour produire des températures autres que celles vraiment relevées? L'un des joueurs ne pourrait-il pas s'introduire sur le site et en modifier les chiffres publiés? Nous verrons par la suite que nous pouvons pallier cette incertitude sur la stabilité et la sécurité de ce qui est inscrit.

Les cours de bourses, les taux de change, les résultats sportifs, le contenu de ce qui est publié par les médias (journaux, radio, télévisions, pages web), sont d'autres sources publiques d'aléas et vérifiables *a posteriori*. Certaines sont assez rapides, mais aucune ne donne une assurance de stabilité supérieure aux données publiées par Météo-France. Avec elles, on aura donc en définitive un aléa public ayant les mêmes imperfections qu'avec Météo-France.

2 AUTRES SOURCES PARTAGEABLES D'ALÉAS

Conscients de l'intérêt de disposer de meilleures sources publiques d'aléas, certains sites internet en proposent. Ainsi, le site random.org rend disponible des nombres aléatoires de toutes sortes depuis 1998.

Ce site, conçu et réalisé par Mads Haahr, du Trinity College, à Dublin, propose des nombres aléatoires qu'il qualifie de «véritables», car

LES FONCTIONS DE HACHAGE

Une fonction de hachage est une fonction qui, à un x donné (une suite de caractères ou un nombre) de longueur quelconque, associe une valeur $f(x)$ de taille fixe, l'« empreinte de x ». Le passage de x à $f(x)$ se fait par une série d'opérations qui commencent en découpant x en morceaux (d'où le nom de hachage). Ces morceaux sont rassemblés et emmêlés de façon à obtenir un brouillage aussi parfait que possible de l'information présente dans x. Pour la fonction classique de hachage SHA-256, la longueur de $f(x)$ est de 256 bits.

Les fonctions de hachage à usage cryptographique, comme SHA-256, ont les propriétés suivantes.
(a) Elles sont « à sens unique » : le passage de x à $f(x)$ est un calcul rapide, mais pour un y donné, trouver x tel que $y = f(x)$ est impossible en pratique.
(b) Il est impossible en pratique de trouver x et x' différents avec $f(x) = f(x')$.
(c) Elles produisent des valeurs assimilables à des valeurs aléatoires uniformes et, en particulier, même si x et x' sont deux suites de caractères n'ayant qu'un seul caractère différent, les valeurs $f(x)$ et $f(x')$ sont sans aucun lien apparent.

Exemple simple. On transforme la donnée x en une suite de 0 et de 1 que l'on découpe en morceaux de longueur 8. Les morceaux sont ensuite additionnés comme des nombres en base 2. On ne garde du résultat que les quatre chiffres centraux :
x = 00010010100101010100100101
→ 00010010 + 10010101 + 00100101 = 11001100
→ $f(x)$ = 0011.
Cet exemple est bien sûr trop simple pour avoir les propriétés (a), (b) et (c).

Exemples d'utilisation.
– Authentifier un utilisateur sans garder son mot de passe *(voir l'illustration ci-contre)*.
– Assurer l'intégrité d'un fichier x. Si l'on dépose un gros fichier sur un serveur, on lui associera son empreinte $f(x)$, beaucoup plus courte. Celui qui téléchargera x s'assurera que x lui parvient sans erreur et en totalité en calculant l'empreinte du fichier qu'il aura reçu, laquelle doit être la même que celle publiée sur le site.
– Engagement d'une donnée sans la révéler. Vous choisissez un nombre que vous ne devez plus changer car, par exemple, vous allez participer à une enchère simultanée ; vous calculez son empreinte et la communiquez à l'organisateur. Le site d'enchère recueille les empreintes des autres participants. Les empreintes sont toutes rendues publiques et ceux qui les ont proposées ne peuvent donc plus rien changer. À cet instant, personne ne connaît les enchères proposées (car f est impossible à inverser), et donc, même si les soumissions ne sont pas simultanées, ceux qui participent ignorent les propositions des autres. La phase d'enchère terminée, chacun révèle son nombre. Le calcul des empreintes des nombres révélés permet de vérifier qu'il n'y a pas eu de changements. Tout s'est donc déroulé comme si chacun avait écrit sa proposition sur un papier et avait placé celui-ci dans une enveloppe cachetée qui n'a été ouverte qu'au dernier moment.

En cryptographie, les fonctions de hachage sont conçues avec soin et soumises à des tests variés. Des compétitions pour concevoir les nouvelles générations de fonctions de hachage sont organisées. Ainsi est née la fonction SHA-3, disponible depuis 2015 (voir https://en.wikipedia.org/wiki/SHA-3).