

ATELIER

Les surprises du hasard





Atelier – Hasard

Un atelier pour faire comprendre aux élèves que l'humain ne sait pas générer correctement du hasard et pour leur expliquer comment l'ordinateur fait.

Matériel :

- Pièces de monnaie
- Tableau
- Feuilles de papier avec grille pour atelier
- Stylos
- Gomme

Durée : 1h



Introductions

Informations

en bleu figurent les moments où les élèves expérimentent, en vert les moments où nous intervenons, en noir le développement et les explications de l'atelier.

L'atelier

Étape 1 : Demander aux élèves la définition du hasard au-delà de l'aspect mathématique une définition du hasard dans la vie de tous les jours. Quelle est la différence avec le terme aléatoire ? Il n'y a pas de grandes différences entre le hasard et l'aléatoire. Selon le dictionnaire Larousse, l'aléatoire est « soumis au hasard » et le hasard est une « circonstance de caractère imprévu ou imprévisible dont les effets peuvent être favorables ou défavorables pour quelqu'un ».

Étape 2 : Expliquer aux élèves que nous allons jouer à « Pile ou face » et qu'ils auront une feuille avec deux grilles de 50 cases dessus, l'une appelée « Tirage n°1 » et l'autre « Tirage n°2 » (La feuille est disponible dans le dossier de l'atelier). Dans un premier temps, les élèves vont inventer un « pile ou face » qu'ils estiment crédible, proche de la réalité. Ce « pile ou face » sera inscrit soit dans les cases correspondant au « Tirage n°1 », soit dans les cases correspondant au « Tirage n°2 ». Ce sont les élèves qui choisissent individuellement où ce tirage sera inscrit.

Étape 3 : Après avoir inventé un tirage, qu'on appellera par la suite « faux tirage », nous distribuons aux élèves une pièce de monnaie (ou ils peuvent les ramener). Cette fois-ci, les élèves réaliseront un vrai « pile ou face » et inscriront le résultat des 50 lancers de pièces dans les cases du tirage restant, soit celles du « Tirage n°2 », soit celles du « Tirage n°1 ».

Étape 4 : Une fois le faux tirage et le vrai tirage réalisés, nous récupérons les feuilles de chaque élève pour les distribuer à un ou une autre de leurs camarades. Chaque élève se retrouve donc avec la feuille d'un ou d'une autre de ses camarades.

Les élèves ont désormais pour objectif de retrouver le vrai tirage et le faux tirage sur la feuille qu'ils viennent de recevoir. Lorsque le faux tirage a été inventé, l'autre objectif était donc aussi de duper ses camarades. Pour cela, il faut créer le faux tirage le plus crédible et réaliste possible pour que l'élève qui reçoit la fiche d'un ou d'une autre se trompe et ne découvre pas la bonne réponse. Il est donc tout aussi important que les élèves choisissent au hasard les cases (Tirage n°1 ou Tirage n°2) où est inscrit le faux tirage et le vrai tirage. Avec la feuille d'un ou d'une camarade sous leurs yeux, les élèves font ainsi un pronostic.



Les élèves créent donc un faux tirage. Puis, nous distribuons une pièce à chaque élève pour créer le vrai tirage. Enfin, les élèves inscrivent leur nom sur la feuille pour qu'on puisse la retrouver une fois dans la main d'un ou d'une de ses camarades. Si besoin, des petits bouts de papier sont à disposition des élèves pour noter leur répartition entre le Tirage n°1 et le Tirage n°2 pour ne pas qu'ils oublient. Pendant ce temps, nous pouvons commencer à tracer au tableau les axes des graphiques qui seront tracés plus tard.

Nous redistribuons les feuilles aléatoirement.

Comment faire pour distinguer un vrai tirage d'un faux tirage ? Ou alors, à quoi ressemblerait un faux tirage et comment reconnaître qu'il est faux ?

Les élèves suggèrent alors de regarder le nombre de piles dans un tirage.

Effectivement, regarder combien de fois le nombre de piles est tombé peut nous aider à trouver le vrai tirage du faux tirage. Par exemple, s'il y a 50 piles et 0 faces, est-ce que le tirage vous paraît réaliste ?

Les élèves suggèrent que le tirage n'est pas réaliste.

Effectivement, ce cas est très rare à se réaliser ! On y reviendra plus tard ! À l'inverse, s'il y a 30 piles et 20 faces, est-ce que le tirage semble réaliste ?

Les élèves suggèrent que le tirage est réaliste.

Il semble en effet plus réaliste car on se rapproche du 50/50, ou du 25/25 dans notre situation. En bref, plus on se rapproche de 25 piles et 25 faces, plus on se rapproche d'un tirage proche de la réalité. Néanmoins, un tirage 30/20 est également proche de la réalité. D'après vous, qu'a pu faire le ou la camarade dont vous avez la feuille ?

Les élèves suggèrent que leur camarade s'est rapproché au maximum du 25/25.

Exactement ! En fait, la plupart du temps, les personnes ont tendance à équilibrer le tirage et c'est normal, on veut tomber proche du 25/25. Néanmoins, à trop vouloir en faire, on peut voir que l'équilibre a été cherché. Pour déterminer un vrai tirage d'un faux, il faut trouver le juste équilibre avec la moyenne (proche de 25/25) sans trop s'éloigner pour autant (un 35/15 est déjà peu réaliste) tout en regardant si on a « forcé » ou non le 25/25.

Comme vous pouvez le voir, sur vos feuilles, il est inscrit « Paramètre 1 » et je vous laisse y inscrire le nombre de piles que vous trouverez dans chaque tirage.

Laisser les élèves compter et inscrire le nombre de pile.

Bien, il reste maintenant un deuxième paramètre à déterminer pour distinguer le vrai du faux ! Quel est-il d'après-vous ?

Les élèves suggèrent le fait d'observer les alternances entre les piles et les faces.

Exact ! Imaginez un tirage avec 25 piles et 25 faces mais celui-ci a une particularité, il est d'abord composé de 25 piles d'affilée puis de 25 faces d'affilée. Ce tirage n'est donc pas très probable, vous ne trouvez pas ?

En effet, ce n'est pas très probable.

À l'inverse, imaginez un tirage où il y d'abord un pile puis un face puis un pile puis un face etc. Est-ce que ce tirage sera probable d'après-vous ?

Les élèves suggèrent que le tirage n'est pas très probable également.

Exactement car il y a trop d'alternances entre les piles et les faces ! Une pièce n'alternerait jamais aussi facilement entre les piles et les faces. Un tirage probable serait par exemple : FFPFPPFPFFPPFP où nous retrouvons une alternance de pile et de face de manière plutôt aléatoire.

Dans « Paramètre 2 », vous allez donc inscrire ce qu'on appelle le « longest run ». Le longest run correspond à la plus longue suite de pile (ou de face) consécutif. Dans notre exemple précédent, le longest run est de 3. Lorsque vous avez 25 piles d'affilée, le longest run est de 25 et quand vous avez une alternance constante de piles et de faces, celui-ci est de 1. Cela nous permettra de savoir s'il y a beaucoup d'alternances ou au contraire, s'il y en a très peu.

Sur le même principe que le 25/25, ici, pour distinguer le vrai du faux tirage, il faut trouver le juste équilibre. Avoir trop d'alternances ou pas assez nous montre un faux tirage. Si vous avez un longest run entre 3 et 6, cela semble crédible. Il est aussi important de savoir que l'humain, qui a toujours tendance à chercher l'équilibre, effectuera plus d'alternances qu'un vrai tirage. Généralement, le tirage avec le plus grand longest run est le vrai (sauf très grand longest run évidemment).

Laisser un temps pour que les élèves comptent et inscrivent les longest run.

D'ailleurs, est-ce qu'une personne parmi vous a deux tirages identiques entre le Tirage n°1 et le Tirage n°2 ?

Les élèves diront que non (Si cela arrive, appelez Minima Gesté).

Normal, car la probabilité qu'un tirage corresponde au votre est de 2^{50} ! Ce qui équivaut à



environ $1,12 \cdot 10^{15}$ ou exactement 1 125 899 906 842 624, ce qui est gigantesque si l'on compare au nombre de tirages fait par votre classe (23 élèves). On peut donc considérer que c'est presque impossible. Pour 10 lancers de pièce, les chances sont déjà de $1 / 1024$. Vous avez donc 1 chance sur 1024 d'avoir le même tirage qu'un de vos camarades sur 10 lancers de pièce.

Pour revenir à la remarque du début, il est donc très rare d'obtenir 50 piles et 0 faces dans un tirage car il n'y a qu'une seule méthode pour avoir 50 piles : c'est de faire.... 50 piles et donc il y a 1 chance sur $1,12 \cdot 10^{15}$.

Alors que pour avoir 25 piles et 25 faces, il y a plusieurs méthodes possibles : 25 piles puis 25 faces, 25 faces puis 25 piles, Une alternance après chaque lancer etc. En tout, il y a $1,26 \cdot 10^{14}$ (ou 126 505 607 505 618) combinaisons possibles permettant de faire 25-25 soit 1 chance sur 8,9 (ou 11,23%). On pourrait trouver ça faible car, statistiquement, seulement 2 ou 3 personnes de votre classe réussiront à faire 25-25 mais ce qu'il y a aussi à retenir c'est qu'il y a 88,13 % de chances de tomber entre 20 et 30 piles inclus.

Maintenant que vous avez compté chaque paramètre et que nous avons vu les probabilités d'apparitions de piles, souhaitez-vous changer votre pronostic ?

Les élèves vont alors changer ou non leur pronostic.

Faire la révélation. Les élèves ont-ils raison ou tort ? Pour la révélation, on va demander à un élève son pronostic puis demander à l'autre élève s'il a eu bon ou non.

Si la majorité des élèves ont raison, cela signifie que les élèves n'ont pas réussi à bien se duper entre eux et donc, que leurs tirages n'étaient pas assez réalistes. À l'inverse, si la majorité des élèves ont tort, cela signifie que les élèves se sont bien dupés entre eux et que leurs tirages étaient réalistes. La majorité du temps, il y a plus de bonnes réponses que de mauvaises, ce qui montre que, sans connaître les règles en avance, l'être humain a des difficultés pour imiter le hasard.

Ce qui est aussi intéressant, c'est qu'il est possible que, pour un tirage donné, tout ce que nous avons vu précédemment sera faux. Par exemple, le vrai tirage aura un longest run de 2 tandis que le faux a un longest run de 6. C'est aussi ça, les probabilités. Sur un grand nombre de tirage, le résultat respectera la loi des grands nombres, c'est-à-dire que les proportions de piles ou de faces par tirage seront respectées au fur et à mesure des tirages. Néanmoins, sur un tirage précis, il peut se passer l'inverse des situations décrites précédemment et on peut obtenir un résultat qui paraît faux, alors qu'il est bien vrai.

Une fois la révélation faite, nous savons donc sur toutes les feuilles où est situé le vrai tirage et le faux tirage. Nous allons donc créer un graphique avec les résultats de chaque paramètre pour visualiser les tendances de tous les tirages (voir **Figure 1** et **Figure 2** qui sont les résultats tirés d'une classe de 23 élèves accueillies au musée).

Comparaison du nombre de piles entre les vrais et les faux tirages

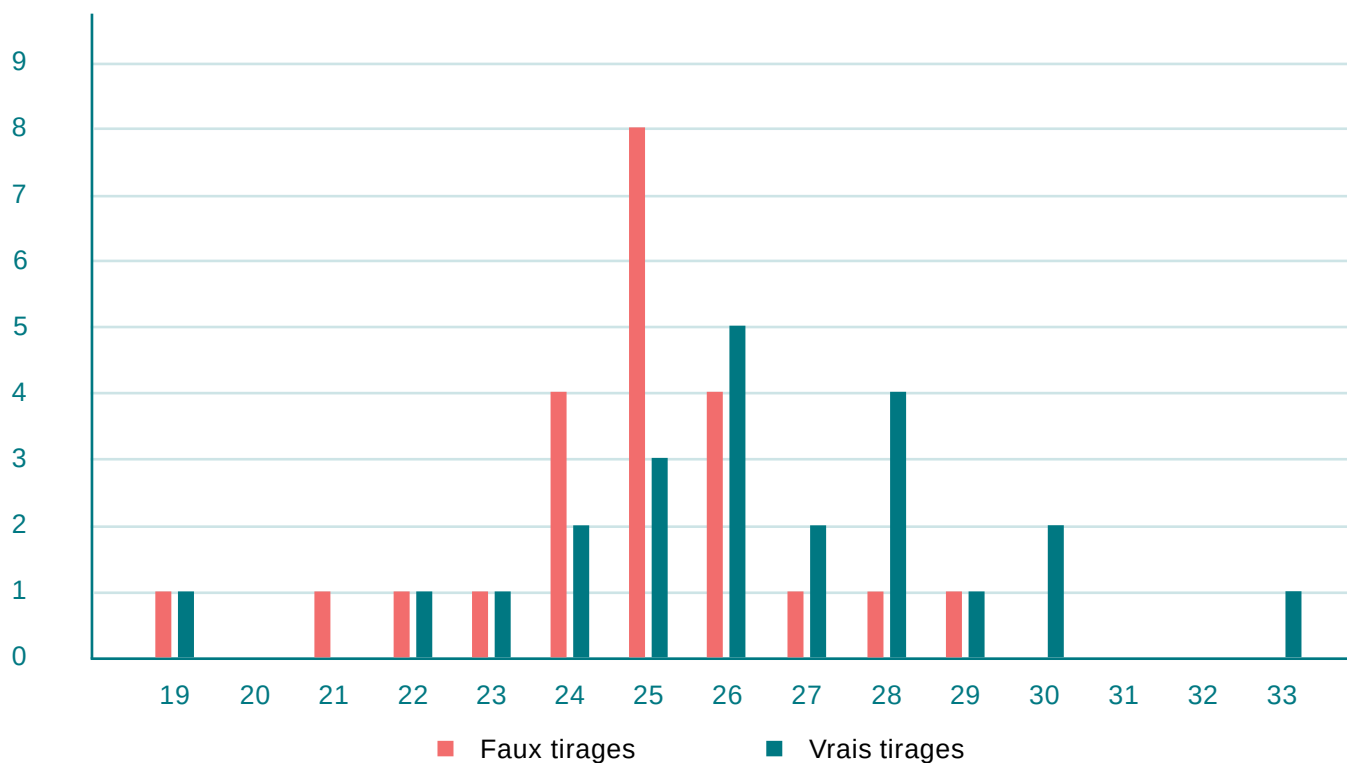


Figure 1: Comparaison du nombre de piles entre les vrais et les faux tirages

Avec ces données et à terme, avec une infinité de données, la courbe du nombre de piles présents dans un tirage suivra **une distribution binomiale** qui tend vers ce qu'on appelle une **courbe de Gauss**. Celle-ci sera centrée en 25 pour les vrais tirages. On pourra alors constater la différence du nombre de piles entre les vrais et les faux tirages. Pour les faux, en général, la courbe sera plus étroite car la majorité des faux tirages ont 24, 25 ou 26 piles. À l'inverse, la courbe des vrais tirages sera plus étendue. Cette comparaison montre bien qu'avec plusieurs tirages différents, les élèves ont souvent tendance à équilibrer et à se rapprocher du 25-25.

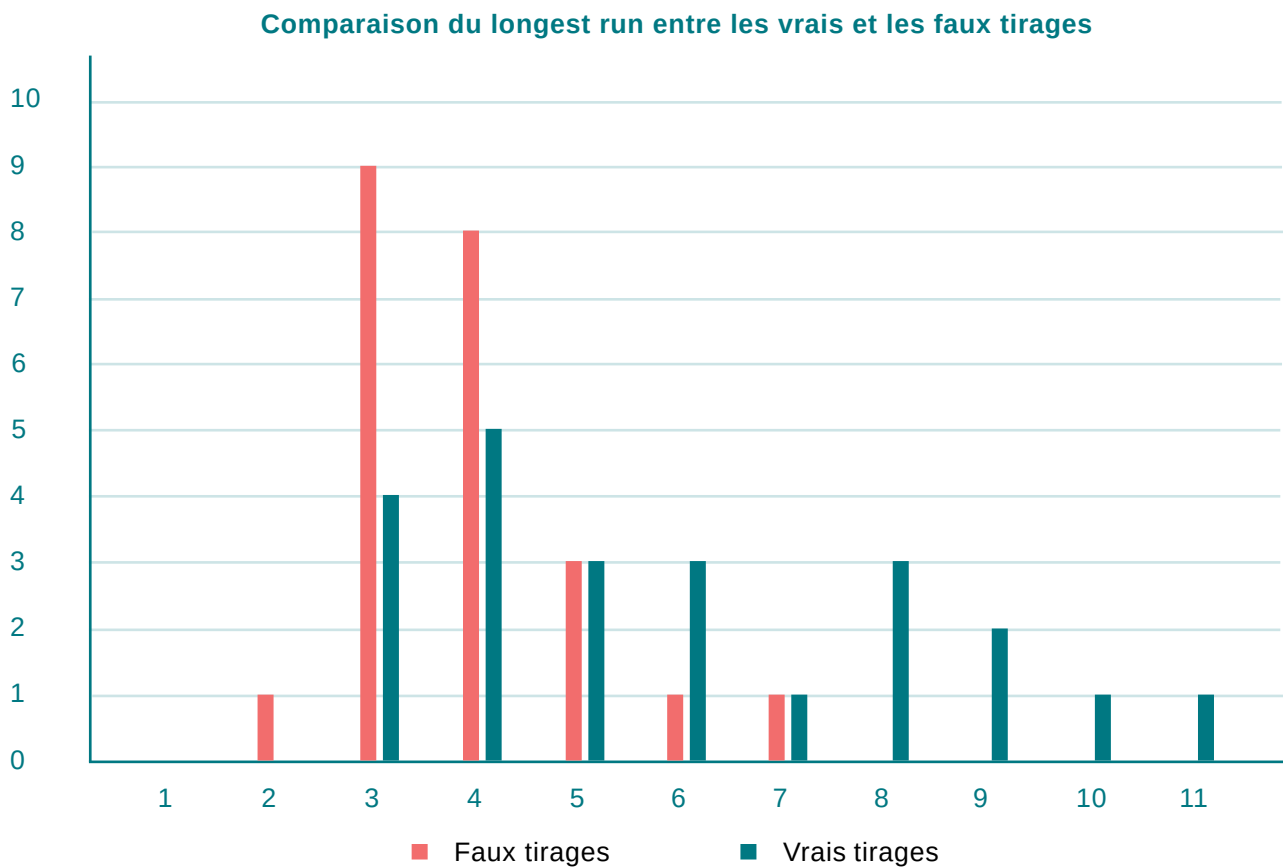


Figure 2 : Comparaison du longest run entre les vrais et les faux tirages

En comparant également les deux tendances pour les longest run, on constatera que la courbe de probabilité sera centrée sur 3 pour les faux tirages et qu'elle sera centrée sur 4 pour les vrais tirages. Aussi, l'étendue sera plus grande pour les vrais que pour les faux tirages ce qui montre bien que les élèves n'osent pas faire de trop grand longest run.

Comment ça marche ?

Explication des résultats

Lorsque l'humain simule le hasard il a tendance à beaucoup alterner les pile/face, créant ainsi des petits « longest run ». Or, quand on étudie les lancers ou les tirages vraiment faits aléatoirement, on constate que les « longest run » sont bien plus élevés. Une manière de distinguer les vrais des faux tirages est donc de regarder la taille des « longest run ». Sur la **Figure 3**, voici une répartition des « longest run » pour un vrai tirage aléatoire. Ici, on regarde la probabilité d'avoir, pour une suite de 50 tirages, un longest run de N , avec N nombre entier.

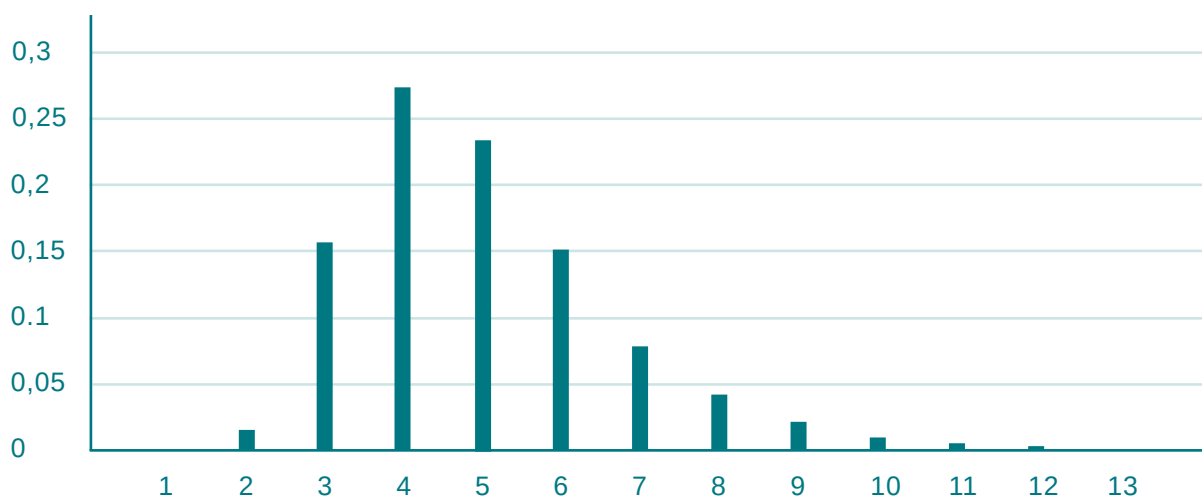


Figure 3 : Répartition du longest run pour un vrai tirage aléatoire

Pour 50 tirages, un longest run de 4 est le plus probable. Si on augmente le nombre de lancers dans la suite, le graphique change et le pic du longest run va tomber sur un N plus grand. À noter qu'un longest run de 10 est plus probable qu'un longest run de 1, qui correspondrait à une alternance parfaite. Pour séparer les groupes, le critère de nombre d'occurrence d'une face ne suffit pas.

Lien avec l'ordinateur ?

Afin de protéger nos données qui sont en ligne, comme par exemple l'envoi d'un message à un ami ou une amie, l'ordinateur va coder nos données en utilisant une clé de chiffrement. Cette clé de chiffrement permet de transformer un message lisible en un message illisible. Pour chaque nouvelle donnée, une nouvelle clé est utilisée. Néanmoins, à chaque fois qu'une clé est créée, un ordinateur utilise le même principe (ou modèle) de chiffrement. En fait, l'ordinateur ne sait pas générer de hasard dans la création de ses clés de chiffrement, il utilise un même modèle. Ainsi, si un attaquant trouve la manière de déchiffrer une clé, il aura la possibilité de déchiffrer toutes les autres clés rapidement. Pour remédier à ce problème, la société Cloudflare utilise une méthode originale pour créer ses clés de chiffrement. Elle utilise des lampes à lave !

Dans une lampe à lave, il y a un liquide et de la cire. La cire étant plus dense que le liquide, elle est donc positionnée au fond de la lampe. Lorsque la lampe est allumée par le dessous, il y aura donc une augmentation de la température. La densité de la cire va diminuer et deviendra inférieure à celle du liquide. Les bulles de cire se mettent alors à monter. Lorsqu'elles s'éloignent de la source de chaleur, leur température baisse, leur densité augmente à nouveau et elles redescendent. C'est un phénomène de convection.

Dans le hall d'accueil du siège de Cloudflare, il est disposé une centaine de lampes avec une caméra dirigée sur chacune des lampes. Ainsi, en fonction des pixels analysés par la caméra, cela modifiera le modèle de création d'une clé ce qui permet de sécuriser solidement les données. Par exemple, pour une lampe à lave rouge et jaune, quand le pixel sera rouge on met un 1, quand le pixel sera jaune, on met un 0 *. Ainsi, on génère une liste binaire complètement au hasard car il est impossible de prédire le mouvement des lampes à laves.

*En réalité, c'est encore plus compliqué car les pixels analysés ne sont pas simplement ceux des lampes à lave mais aussi ceux de tout l'environnement autour (changement de luminosité lié à la météo et à l'heure de la journée, personne qui se positionne devant le mur etc.).



Pour s'amuser

Voici un site qui permet de savoir les probabilités d'apparition de pile ou de faces en fonction du nombre de lancers : <https://www.omnicalculator.com/fr/statistiques/calculateur-pile-ou-face>. C'est ici que j'ai trouvé les chiffres précis des probabilités.

Loi binomiale sur Wikipédia : https://fr.wikipedia.org/wiki/Loi_binomiale

Article qui explique la distribution de probabilité du longest run :

<https://www.csun.edu/~hcmth031/tlroh.pdf>

Lien au PDF dans le Cloud : <https://cloud.ihp.fr/f/3502203>

Sources :

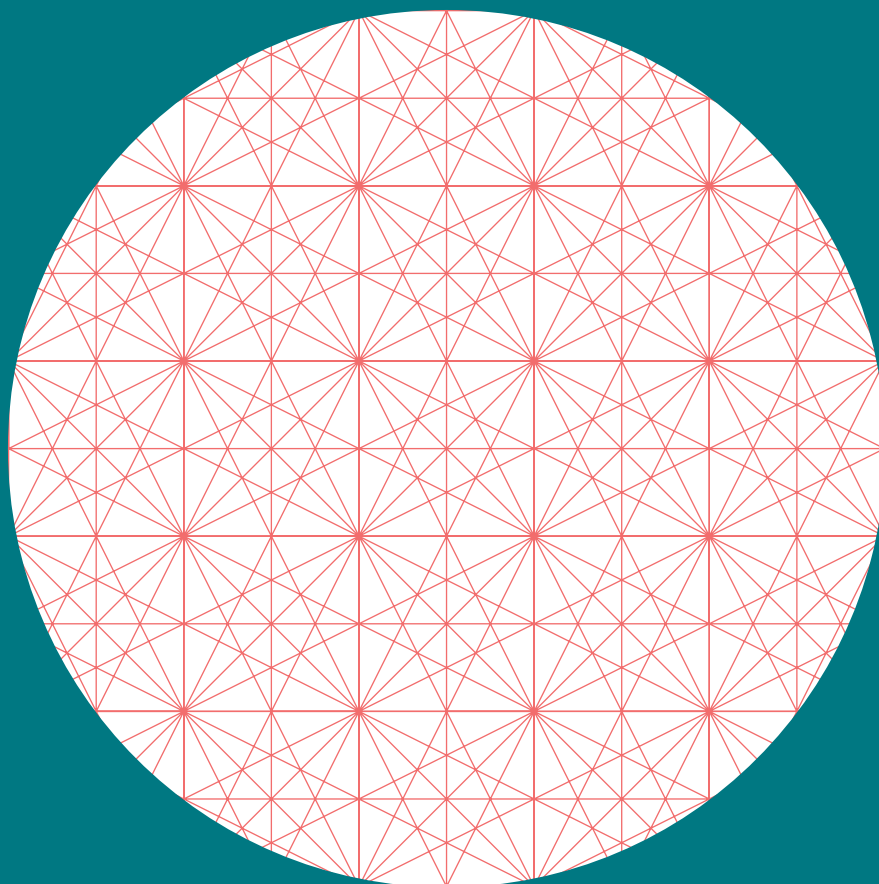
Comment les lampes à lave contribuent-elles au chiffrement Internet ? | Cloudflare

<https://www.entrust.com/fr/resources/learn/how-to-manage-encryption-keys>

<https://www.okta.com/fr-fr/identity-101/password-encryption/>

Pour aller plus loin. Il y a un troisième paramètre que l'on peut considérer après le nombre de pile et le longest run, qui s'appelle l'incompressibilité. J'en parle car les élèves ont parfois une intuition de ce concept, lorsqu'ils disent qu'une série « trop régulière » (par exemple PPPFFFPPPPFF) serait suspecte. On peut donc leur mentionner qu'on peut aussi quantifier cette « régularité » et l'utiliser pour distinguer les vrais des faux tirages.

L'incompressibilité est un concept lié à la théorie de l'information et correspond grosso modo au nombre d'instructions qui seraient nécessaires pour générer la suite. Une alternance parfaite de pile ou face serait « résumée » par la consigne « écrire P, écrire F, répéter les 2 instructions précédentes 25 fois », alors qu'une suite parfaitement aléatoire est impossible à résumer en seulement quelques instructions.



Institut Henri Poincaré | Maison Poincaré
11, rue Pierre et Marie Curie, 75005 Paris

profs-maison-poincare@ihp.fr
01 44 27 64 73
maison-poincare.fr