# Combinatoire et dénombrement
## Problème de recherche : le mot de passe incassable

Un pirate essaie tous les mots de passe possibles (attaque par « force brute ») avec un ordinateur capable de tester $10^{10}$ mots de passe par seconde. Un clavier permet de taper 95 caractères différents (lettres minuscules et majuscules, chiffres, symboles, espace).

### La mission

1. Combien existe-t-il de mots de passe de 8 caractères ? Combien de temps faut-il au pirate, au pire, pour tous les tester ?
2. Un site impose « au moins un chiffre » dans les mots de passe de 8 caractères. Combien de mots de passe restent autorisés ? Cette règle rend-elle la tâche du pirate plus difficile ?
3. La méthode *Diceware* consiste à tirer au hasard 5 mots dans une liste de 7 776 mots courants (avec répétition possible), par exemple « tigre cuivre rondo plage vélo ». Est-ce plus sûr qu'un mot de passe de 8 caractères ?

### Pour aller plus loin

Pourquoi la liste Diceware compte-t-elle exactement 7 776 mots ? Que vaut un mot de passe de 12 lettres minuscules ?

### Coups de pouce

Bloqué ? Des indices progressifs sont disponibles en ligne. N'en ouvrir qu'un à la fois, et seulement après avoir cherché !

# Éléments de correction

## 1. Mots de passe de 8 caractères

Un mot de passe est un 8-uplet d'éléments d'un ensemble à 95 éléments : il y en a

$$95^8 \approx 6{,}63 \times 10^{15}.$$

Temps au pire : $\frac{6{,}63\times10^{15}}{10^{10}} \approx 6{,}63 \times 10^5$ s, soit environ **7,7 jours**. (En moyenne, la moitié.)

## 2. Au moins un chiffre

On passe par le complémentaire : les mots de passe **sans** chiffre utilisent 85 caractères, il y en a $85^8$. Donc

$$95^8 - 85^8 \approx 3{,}91 \times 10^{15} \text{ mots de passe autorisés,}$$

soit environ 59 % des mots de passe possibles. Paradoxe : si le pirate connaît la règle, **elle lui facilite la tâche** (41 % de candidats en moins) ! Son intérêt réel est ailleurs : elle empêche les mots de passe trop simples (« motdepas »), que le pirate teste en premier avec un dictionnaire.

## 3. Diceware

Un tirage est un 5-uplet de mots parmi 7 776 : $7\,776^5 \approx 2{,}84 \times 10^{19}$ possibilités. Au pire : $2{,}84 \times 10^9$ s, soit environ **90 ans**. Une phrase de 5 mots simples est environ **4 300 fois** plus résistante qu'un mot de passe de 8 caractères compliqués, et bien plus facile à retenir. (Hypothèse essentielle : les mots sont vraiment tirés au hasard, pas choisis.)

## Pour aller plus loin

$7\,776 = 6^5$ : on choisit chaque mot en lançant 5 dés à six faces (par exemple 3-1-6-2-4 donne le numéro du mot dans la liste). Douze lettres minuscules : $26^{12} \approx 9{,}5 \times 10^{16}$, soit environ **110 jours** au pire : la longueur compte plus que la variété des caractères. En informatique, on mesure la force d'un mot de passe en bits : $\log_2(95^8) \approx 52{,}6$ bits contre $\log_2(7\,776^5) \approx 64{,}6$ bits (enrichissement).

## Ce qu'on a utilisé du chapitre

— Nombre de $k$-uplets d'un ensemble à $n$ éléments : $n^k$.
— Dénombrement par passage au complémentaire.