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 !