CORRIGE DM : PUISSANCES ET ECRITURE

0. Écritures de nombres

a. 0 ;1 ;2 ;3 ;4 ;5 ;6 ;7;8 ;9 sont tout autant des chiffres que des nombres. Ce sont des nombres à un chiffre. Tout comme, en français, dans la phrase « j'y vais », 'y' est un mot à une seule lettre.

b. 00 ;01 ;02;03;04;05;06;07;08;09 ; 10 ; 11 … 99 sont 100 écritures différentes.
Il y en a 99 de 01 à 99 et il ne faut pas oublier 00, ce qui fait 100 en tout. $100 = 10^2$
Autre démarche : il y a 10 possibilités pour le premier chiffre, 10 pour le deuxième :
ce qui donne $10 \times 10 = 10^2 = 100$ écritures différentes.

1. Le cadenas à code

a. Il y a 10 possibilités pour chaque chiffre. Ce qui fait en tout $10 \times 10 \times 10 = 10^3$ codes différents.

Il y a 1000 codes. Chaque test prend au voleur une seconde. Cela va lui prendre 1000 secondes.

1000 s = $\frac{1000}{60}$ min ≈ 16,67 min 0,67 min = 0,67 × 60 s = 40,2 s

Le voleur mettra environ 16 min et 40 secondes. C'est presque faisable en une récréation.

b. On rajoute un chiffre. Cela va donner $10 \times 10 \times 10 \times 10 = 10^4$ codes différents.

Le voleur mettra 10 fois plus de temps, soit 10 000 secondes. Ce qui fait environ 166,67 min, autrement dit : 2 heures 46 minutes et 40 secondes.

c. On rajoute encore un chiffre. Cela va donner $10 \times 10 \times 10 \times 10 \times 10 = 10^5$ codes différents.

Il va mettre encore 10 fois plus de temps, 100 000 secondes. Plus de 27 heures.

2. Adresses IP :

a. De 1 à 255, il y a 255 nombres. Et on n'oublie pas le zéro, ce qui fait 256 nombres.

b. Les adresses vont de 0.0.0.0 à 255.255.255.255. Il y a 256^4 adresses différentes.

c. $256^4 = 4\ 294\ 967\ 296$. Il y a plus de 7 milliards d'être humains sur Terre, et en 2020 il y a environ 30 milliards d'objets connectés à Internet. Cela a été rendu possible en passant à un nouveau système d'adressage : IPV6, qui permet d'avoir beaucoup plus d'adresses.

3. Les mots de passe sur internet

a. Il y a 26 lettres dans l'alphabet.
b1. 3 caractères, uniquement des chiffres. On retrouve le cadenas à code. $10 \times 10 \times 10 = 10^3 = 1000$
On peut former 10^3 chaînes de caractères différentes.
b2. C'est comme si on avait un cadenas à code avec des lettres. $26 \times 26 \times 26 = 26^3 = 17576$
On peut former 26^3 chaînes de caractères différentes.
b3. Pour chaque caractère les possibilités sont a,b,c,…,z,0,1,2,...,9. 26 + 10 = 36.
$36^3 = 46656$. On peut former 36^3 chaînes de caractères différentes.

c. L'attaque par force brute est l'équivalent numérique de la stratégie du voleur pour le cadenas à code ; On n'essaye pas de deviner le code, on teste bêtement toutes les possibilités, car on sait qu'en les essayant toutes, on finira par tomber sur la bonne.

c1. Le pirate va mettre $\frac{1000}{30\,000\,000}$ secondes.

Avec la notation scientifique : $\frac{1\times10^{3}}{3\times10^{7}} = \frac{1}{3}\times10^{-4} \approx 0{,}33\times10^{-4} \approx 3{,}33\times10^{-5}$

Le pirate mettra environ 333 millionièmes de secondes pour tester toutes les chaînes de caractères de longueur 3 formées uniquement de chiffres.

c2.Le pirate va mettre $\frac{26^{3}}{30\times10^{6}}$ secondes.

$\frac{26^{3}}{30\times10^{6}} \approx \frac{1{,}76\times10^{4}}{3\times10^{7}} = \frac{1{,}76}{3}\times10^{-3} = \frac{1{,}76}{3}\times10^{-3} = 0{,}586\times10^{-3} = 5{,}86\times10^{-4}$

Ce qui fait environ $5{,}86 \times 10^{-4}$ secondes. Donc environ 590 microsecondes.

C3. Le pirate va mettre $\frac{36^{3}}{30\times10^{6}}$ secondes, ce qui fait environ 1,56 millisecondes.

Conclusion : les chaînes de caractère courtes sont testées en un clin d'oeil.

d. **Pour se protéger, on choisit un mot de passe long, qui fait 20 caractères.**

$26^{20} \approx 1{,}993 \times 10^{28}$

$\frac{26^{20}}{30\times10^{6}} \approx \frac{1{,}993\times10^{28}}{3\times10^{7}} = \frac{1{,}993}{3}\times10^{21} = 6{,}64\times10^{20}$.

Le pirate mettre $6{,}64 \times 10^{20}$ secondes,

$6{,}64\times10^{20}$ secondes, ça fait combien d'années ?

Une année c'est 365 x 24 x 60 x 60 secondes. $365 \times 24 \times 60 \times 60 = 31\,536\,000 = 3{,}15 \times 10^{7}$

$\frac{6{,}64\times10^{20}}{3{,}15\times10^{7}} \approx 2 \times 10^{13}$. Le pirate mettra environ 20 mille milliards d'années.

Si j'étais lui, je chercherais une autre technique pour les mots de passe longs.

A réfléchir tranquillement (*cette question ne fait pas partie du DM*):
Peut-on vraiment se sentir mieux protégé maintenant que l'on a mis un mot de passe long ?
Une piste de réflexion :

Imaginons que le pirate ait une liste des mots français les plus utilisés.
Il peut essayer de fabriquer des chaînes de caractères en mettant à la suite différents mots dans n'importe quel ordre.
Fabriquer une chaîne de caractères en mettant à la suite des chaînes de caractères s'appelle **concaténer** les chaînes. On note souvent les chaînes de caractère entre apostrophes ".

Exemple : à partir de "chien" et "mechant" on fabrique "chienmechant".

S'il a dans sa liste "mon", "mot", "de", "passe", "est" et "fort", il pourra fabriquer par exemple :

"monpassefort", "mondemon", "demonfortpasseest", et aussi "monmotdepasseestfort".

Donc, utiliser des mots courants n'est pas forcément une bonne idée.
Les élèves qui font des fautes d'orthographe sont privilégiés car s'ils font des fautes dans leur mot de passe, les mots « pièce de puzzle » à utiliser seront plus compliqués à rassembler.

Exemple : monmautdepasséplusfaur