

Exercice 1 : Combinaisons (coloriages)

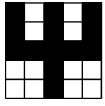
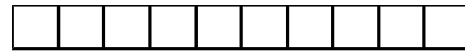
1) On dispose de 3 cases. Chaque case peut être coloriée en rouge ou en vert (donc 2 couleurs). Réaliser tous les coloriages possibles. Combien y en a-t-il ? (*remarque : l'ordre importe... R-V-V n'est pas V-V-R*). Mettre ce nombre sous la forme a^n .



2) On dispose maintenant de 2 cases mais de 3 couleurs. Mêmes questions qu'au 1)



3) Si l'on dispose d'une bande de 10 cases, que l'on peut colorier de 8 couleurs différentes, combien de coloriages sont possibles ? (*ne pas les réaliser !*)



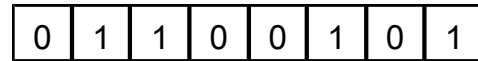
4) Combien existe-il d'images de 5×5 pixels noirs et blancs ?

5) Combien existe-il d'images de 6×6 pixels codés sur 256 couleurs. Est-ce plus que le nombre d'atomes dans l'univers ? (10^{80})

Exercice 2 : Langage binaire

Les ordinateurs utilisent une base binaire pour compter, c'est-à-dire qu'ils n'utilisent que deux symboles (représentés par 0 et 1). Les premiers nombres sont 0, 1, 10, 11, 100, 101, etc. avec $1=1$, $10_2=2$, $11_2=3$, $100_2=4$, etc.

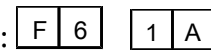
Un octet est la donnée de huit « 0 » ou « 1 », par exemple :



- 1) Combien d'octets différents existe-il ?
- 2) Quelle est la valeur de 1000_2 en base 10 ?

Une autre manière d'écrire en informatique est l'hexadécimal, qui regroupe cette fois 16 symboles : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.

3) Combien de combinaison existe-il pour deux caractères ? comme par exemple :



4) Pourquoi peut-on dire qu'un octet est la donnée de deux caractères hexadécimaux ?

Exercice 3 : Mots de passe

Les mots de passe sont maintenant utilisés dans la vie de tous les jours, notamment pour accéder à du contenu sécurisé (email, compte sur un site, etc.). Nous allons nous intéresser à la sécurité des mots de passe. Répondre en utilisant une écriture scientifique : $a \times 10^n$ avec deux chiffres après la virgule pour a .

1) Combien de mots de passe existe-il comportant...

- a) ... 4 caractères minuscules, comme par exemple : « abcd », « pmpw », « allo », « dede » ?
- b) ... 4 caractères majuscules et/ou minuscules, comme « SaLu », « JmPL », « HEHO » ?
- c) ... 5 caractères minuscules ?

2) Un pirate possède un outil permettant de tester 7100 mots de passe par seconde sur un document protégé par mot de passe.

- a) Combien de temps mettra-il pour tester tous les mots de passe comportant 4 minuscules ? (en secondes)
- b) Pour tester tous ceux à 4 minuscules ou majuscules ? (en minutes)

3) Nous allons maintenant écrire des mots de passe pouvant comporter 80 caractères alphanumériques (les 26 minuscules + les 26 majuscules + les 10 chiffres + 18 caractères spéciaux comme @ ! #)

- a) Combien y a-t-il de mots de passe alphanumériques à 6 caractères (comme « y#KL01 » ou « m@34Tz ») ?
- b) Combien d'années le pirate mettrait-il pour tester toutes les combinaisons ? et la moitié ?

Remarque : en l'état actuel des technologies, 8 caractères semblent être le minimum pour être sécurisé. Cependant, beaucoup de gens utilisent des mots de passe simples comme « azerty12 » ou « iloveyou ». Ces mots de passe peuvent être facilement crackés car proches de mots existants. Un bon mot de passe doit être difficile à deviner, proche de l'aléatoire : « k#mL85@f » ou « ZuP986#! », ou alors être constitués de mots sans rapport : « C@stor24Kirikou » ou « 30TortuesTordues() »