Entropie d'un mot de passe

Lycée Carcouët

24 novembre 2022

Devinette : mot de passe à un caractère

Je pense à un entier entre 0 et 7 (parmi 0 1 2 3 4 5 6 7).

Posez-moi des questions pour le deviner.

Je ne peux répondre que par OUI ou NON.

Devinette : mot de passe à un caractère

Je pense à un entier entre 0 et 7 (parmi 0 1 2 3 4 5 6 7).

Posez-moi des questions pour le deviner.

Je ne peux répondre que par OUI ou NON.

Combien de questions suffisent ?

Réponse

3 questions suffisent pour trouver un entier M,
$M \in \{0{,}1; 2; 3; 4; 5; 6; 7\}$.

Exemple :

1. M est-il inférieur ou égal à 3,5 ? OUI
2. M est-il inférieur ou égal à 1,5 ? OUI
3. M est-il égal à 1 ? NON

C'est 0.

Passage en binaire

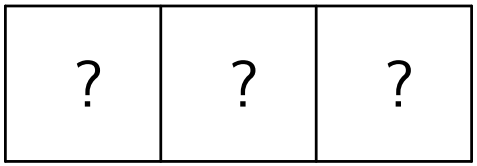
Pas vraiment convaincu par le nombre suffisant de questions égal à 3 ?

Passons en binaire.
Pour représenter 8 chiffres, 3 bits suffisent

0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

Il devient évident qu'il faut poser 3 questions : une sur chaque bit. Chacun est-il égal à 0 ou 1 ?

Entropie/information



En théorie de l'information, ce 3 s'appelle l'**entropie** de notre nombre à deviner.

Notre mot de passe à 8 caractères possibles a une entropie de 3 bits (l'unité d'entropie est le bit).

3 bits est la **quantité d'information** acquise lorsque le mot de passe devient connu.

Remarque

Dans l'exemple précédent, on s'est arrangé pour utiliser 8 caractères.

$$8 = 2^3$$

Code de carte bleue

Exemples : 4567 7102
On utilise 4 caractères choisis parmi les 10 chiffres (de 0 à 9).

Il y a donc 10^4 codes possibles.

$$2^{13} < 10^4 \leqslant 2^{14}$$

Pour représenter le code en binaire, il faudra entre 13 et 14 bits.

L'entropie d'un code de carte bleue est comprise entre 13 et 14 bits.

(pour trouver 13 et 14 sans tâtonner, il faut connaître le logarithme à base 2 : $\log_2\left(10^4\right) \simeq 13{,}29$)

Entropie d'un mot de passe égale à 80 bits

Pour un mot de passe de longueur L utilisant seulement les 10 chiffres (de 0 à 9), on a 10^L mots de passe à essayer (au maximum, si on veut le deviner)

Il faut trouver L tel que

$$10^L \geqslant 2^{80}$$

$2^{80} \simeq 1{,}21 \times 10^{24}$ donc $L = 25$.

Pour avoir une entropie de 80 bits, il faut un mot de passe de longueur 25.

Entropie d'un mot de passe égale à 80 bits

Pour un mot de passe de longueur L utilisant 62 caractères (les 26 lettres minuscules de a à z, les 26 majuscules de A à Z et les 10 chiffres de 0 à 9), on a 62^L mots de passe à essayer (au maximum, si on veut le deviner)

Il faut trouver L tel que $62^L \geqslant 2^{80}$.
On trouve $L = 14$.

Il faut un mot de passe de longueur 14.

(si on connaît $\log_2$, pas besoin de tâtonner : $L \geqslant \dfrac{80}{\log_2(62)} \simeq 13{,}43$)

Supplément

La définition générale de l'entropie fait appel à plus de notions mathématiques.
Pour un système à n états possibles x_1, ..., x_n de probabilités p_1, ..., p_n :

x_i	x_1	x_2	...	x_n
p_i	p_1	p_2	...	p_n

l'entropie H est

$$H = -\sum_{i=1}^{n} p_i \log p_i$$

(log désigne $\log_2$, le logarithme à base 2)

Supplément

Pour un système à deux états équiprobables :

x_1	x_2
$\frac{1}{2}$	$\frac{1}{2}$

l'entropie H est

$$\begin{aligned} H &= -\left(\frac{1}{2}\log\frac{1}{2} + \frac{1}{2}\log\frac{1}{2}\right) \\ &= -\left(-\frac{1}{2}\underbrace{\log 2}_{1} - \frac{1}{2}\underbrace{\log 2}_{1}\right) \\ &= 1 \end{aligned}$$

C'est pourquoi l'entropie d'un mot de passe que l'on peut écrire en binaire sur un bit est 1 (bit) !

Supplément

Pour un mot de passe qui s'écrit en binaire sur n bits (où pour chaque bit, 0 et 1 sont équiprobables), l'entropie est

$$\begin{aligned} H &= -\sum_{i=1}^{n} p_i \log p_i \\ &= -\sum_{i=1}^{n} \frac{1}{n} \log \frac{1}{n} \\ &= -n\frac{1}{n} \log \frac{1}{n} \\ H &= \log n \end{aligned}$$