Nouvelles d’une taupe modèle

Par Kylie Ravera

L’Institut Intergalactique est le temple de l’excellence où exerce le redouté professeur Phi. Kylie Ravera nous raconte leurs aventures.

Un joyeux crypto-anniversaire

L’Institut Intergalactique est certes un temple de l’excellence qui invite au travail, au sérieux et à la performance, les élèves qu’il accueille n’en sont pas moins des jeunes gens comme les autres qui éprouvent parfois le besoin de socialiser. Une tradition perdure ainsi depuis des années : celle du gâteau d’anniversaire. Chaque élève célèbre sa naissance en amenant le jour J un goûter pour le reste de sa classe.

Aujourd’hui, c’est au tour de Delta de régaler ses 39 camarades avec un cake aux noix de Centaure. La pause est bienvenue : elle précède un cours de crypto-mathématique dispensé par le redoutable Professeur Phi,

Une part de cake à la main, Epsilon s’approche d’Oméga qui en est rendu à faire la chasse aux miettes égarées sur son pull.

— Déjà fini ?, lui demande-t-elle avec un sourire.

Oméga est réputé pour apprécier les bonnes choses, comme en témoigne son embonpoint.

— Oui, soupire-t-il tout en lorgnant sur le gâteau de sa camarade : je trouve quand même qu’une seule part, c’est trop peu…

Epsilon se hâte d’engloutir sa dernière bouchée.

— Patience, répond-elle, il y aura bien un jour où deux élèves fêteront leur anniversaire en même temps. Cette fois-là, ce sera double ration !

Oméga fronce les sourcils.

— J'en doute. Nous ne sommes que 40 dans la classe. Il est peu probable que 2 élèves aient leur anniversaire qui tombe le même jour.[1] On serait autour de 180, peut-être…

Il se mord aussitôt les lèvres, mais il est trop tard. Epsilon s'est déjà emparé d'une feuille et d'un crayon et Oméga sait bien que la jeune fille, autrement discrète et sympathique, ne plaisante pas avec ces choses-là. Il lève les yeux au ciel et se force malgré tout à suivre la démonstration :

— Calculons la probabilité pour que tous les anniversaires des élèves de la classe tombent un jour différent, propose-t-elle. Si on considère 2 élèves, la date d'anniversaire du 1er étant fixée, il ne reste plus que 365-1 dates possibles pour le 2ème. Cette probabilité est donc : $p_2 = \frac{365-1}{365}$ Si on considère un 3ème élève, ce dernier n'a plus que le choix entre 365-2 dates possibles pour un cas favorable, et la probabilité devient : $p_3 = \left(\frac{365-1}{365}\right) \times \left(\frac{365-2}{365}\right)$

Au final, pour une classe de 40 élèves :

$$p_{40} = \left(\frac{365-1}{365}\right) \times \left(\frac{365-2}{365}\right) \times \ldots \times \left(\frac{365-39}{365}\right) = \frac{365!}{(365-40)!} \times \frac{1}{365^{40}}$$

— Super, maugrée Oméga.

Epsilon l'ignore.

— Pour trouver la probabilité qu'au moins 2 élèves de la classe fêtent leur anniversaire le même jour, ce qui est le complémentaire de la proposition précédente, il suffit de retirer cette probabilité à 1.

Elle pianote rapidement sur la calculatrice fixée à son poignet.

— En valeur numérique, conclut-elle, cela nous donne $P_{40} = 1 - p_{40} = 89\%$. Tu vois, j'ai de grandes chances d'avoir raison !

[1] Pour d'obscures raisons historiques dont l'origine se perd dans la nuit des temps, une année à l'Institut Intergalactique compte 365 jours. Et les politiques successives visant à travailler plus ont conduit à la suppression des week-ends pour les préparationnaires.

Cette fois, Oméga écarquille les yeux.

— C’est dingue, souffle-t-il, cherchant en vain une faille dans la démonstration.

Intuitivement, il aurait juré qu’il fallait bien plus d’élèves dans la classe pour pouvoir espérer avoir un jour droit à deux parts de gâteau.

— En fait, ajoute Epsilon qui a continué à gribouiller des équations sur son papier, en calculant cette probabilité pour différents effectifs, on se rend compte qu’il suffit d’une classe de 23 élèves pour qu’elle soit supérieure à ½. Si on était 60 comme chez nos amis littéraires, elle passerait à plus de 99%...

Cette passionnante conversation prend brusquement fin quand le Professeur Phi entre dans la salle. Il affiche un sourire carnassier et un air satisfait.

— Mesdemoiselles, messieurs, pour vous accompagner dans votre digestion, je vous propose un petit devoir sur table, annonce-t-il dans un silence de mort. Il va porter sur les fonctions de hachage que nous avons étudiées cette semaine. La question est simple : en considérant des résumés sur b bits, combien un attaquant qui cherche à établir une collision doit-il essayer de textes avant de tomber sur un résumé déjà sorti avec une probabilité d’au moins un demi ? Vous avez une heure.

Au milieu du concert de soupirs, Oméga se prend la tête dans les mains. Son regard croise alors celui d’Epsilon qui lui adresse un clin d’œil en indiquant les feuillets qu’elle vient de noircir. Peu à peu, le visage d’Oméga s’éclaire et il commence à rédiger sa réponse.

Et vous, cher lecteur, saurez-vous faire le lien entre la question du Professeur Phi et le paradoxe des anniversaires ?

Solution

Le problème qu'Epsilon vient de résoudre permet en fait de répondre à la question du Professeur Phi. Une fonction de hachage qui conduit à un résumé de *b* bits propose 2^b résumés différents. Si l'on considère *k* textes distincts, une collision se produit si au moins deux de ces textes produisent le même résumé. On cherche donc *k* fonction de *b* tel que la probabilité d'une collision soit supérieure à ½. Tout se passe comme si l'on cherchait le nombre d'élèves d'une classe pour que la probabilité que l'anniversaire de deux d'entre eux tombe le même jour, parmi cette fois 2^b dates possibles, soit supérieure à ½ !

Un peu de calcul : on a vu que $P_k = 1 - \prod_{i=0}^{k-1}(1 - \frac{i}{2^b})$. Pour résoudre l'inégalité $P_k > 1/2$, on utilise un développement limité au voisinage de 0 : $1 - x \approx e^{-x}$ pour obtenir

$$P_k \approx 1 - \prod_{i=0}^{k-1} e^{-\frac{i}{2^b}} = 1 - e^{-\sum_{i=0}^{k-1}\frac{i}{2^b}} = 1 - e^{-\frac{\sum_{i=0}^{k-1} i}{2^b}} = 1 - e^{-\frac{k(k-1)}{2\times 2^b}}$$

On trouve simplement la condition : $k > \frac{1+\sqrt{1+8\ln 2\times 2^b}}{2}$ Une application numérique montre qu'il faut viser au moins 128 bits pour la taille du résumé si on souhaite donner du fil à retordre à l'attaquant. Avec un résumé sur 8 bits, à peine une vingtaine de textes suffisent pour obtenir une collision avec plus d'une chance sur 2…