Rédacteur : Élie AOUAD

Attaque par les Dates d'Anniversaire

L'une des premières attaques que j'ai appris il y a plusieurs années est l'attaque par les dates d'anniversaire qui se résume à la problématique suivante : Dans une assemblée quel est le nombre minimal de personnes présentes pour qu'au moins deux personnes aient la même date d'anniversaire (jour et mois) avec une probabilité de 50%.

1) Je vais commencer par donner la formule mathématique en considérant que L est le nombre de jours de l'année:

a) La probabilité P(n) pour qu'au moins deux personnes aient la même fate d'anniversaire dans une assemblée de n personnes=

P(n) = 1 - probabilité que toutes les personnes aient des dates d'anniversaires différentes. pp(n)

b) La probabilité pp (n) pour que n personnes aient des dates d'anniversaires différentes =

*(L-n+1)/L * pp(n-1)*

avec pp(2) = L-1/L

=> **pp(n) = ((L-n+1)*(L-n+2)*....(L-1))/ L exp(n-1)**

et P(n) = 1 - pp(n) qui est une fonction croissante en fonction de n et décroissante en fonction L .

Pour les grandes valeurs de L, P(n) est presque égal à n*n /2L avec n<<L

2) et je vais continuer par un tableau de simulation:

Avec L = 365

n	2	5	10	15	20	22	23
pp(n)	0,997	0,973	0,883	0,747	0,588	0,524	0,493
P(n)	0,003	0,027	0,117	0,253	0,412	0,476	0,507

Donc il faut 23 personnes pour avoir qu'au moins deux personnes aient la même date d'anniversaire avec une probabilité de 50% !!!

3) L'application de cette formule dans le monde cryptographique définit l'attaque par les dates d'anniversaires: la date correspond au sceau et que les personnes correspondent aux données scellées. Deux messages avec un même sceau correspondent à une collision. Cette fréquence est fortement croissante avec le nombre de messages . D'où l'une des caractéristiques d'un bon algorithme de scellement est de diminuer la fréquence des collisions et d'offrir une bonne taille de sceau (128 ou 160 bits actuellement) ; qui dans le cas des dates d'anniversaire consiste à prendre en compte l'année et lieu de naissance aussi.