Author : Élie AOUAD

Birthdays Attack

One of the first attacks that I learned was the birthdays attack. What is the necessary number of persons in a group in order to have at least two persons with the same birthday (day and month) with a probability of 50%.

1) I will begin with the mathematical formula by considering that L is the number of days in one year:

a) The probability P(n) for that at least two persons have the same birthday is given by =

P(n) = 1 - probability that all persons have different birthdays pp(n)

b) The probability pp (n) that n persons have different birthdays =

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

with pp(2) = L-1/L

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

and P(n) = 1 - pp(n) which increases with n and decreases with L.

For big L, P(n) almost equals to square(n)/2L with n<<L.

2) and I shall continue with the following simulation table :

with 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

Only 23 persons are needed in order to have at least two persons with the same birthday with a probability of 50% !!!

3) By applying the formula to a seal (digest) corresponding to the date and the sealed(hashed) message corresponding to persons we obtain the Birthdays Attack.Two messages with the same seal or digest give a collision . The frequency of the collisions strongly increases with the number of messages. A good hash algorithm reduces collision frequency by increasing the seal/digest length (128 or 160 bits actually) ; which is in the case of birthdays to consider the year and place of birth.