(1) Birthday Paradox - Generalized Problem

(2) Key Distribution

Reg Birth Paradox

prob k diff birthdays out of k

$$\frac{365}{365} \times \frac{364}{365} \times \frac{363}{365} \times \cdots \frac{365-k+1}{365}$$ ← Sample Space is 365^k

for this problem

Sample Space = 365^k, k = total people $c_1+c_2+c_3+\cdots c_n$

Goal: Count how many items in sample space are "successes"?

3, 2, 1, 1, 1, 1, 1

A C D B E A B F A G ⇒ # strings ⇒ $\frac{10!}{3!2!1!1!1!1!1!}$

→ A A A B B C D E F G

→ A A A B B D C E F G

A = 365 D = 362
B = 364 E = 361
C = 363 F = 360
G = 359

$$\#\text{Success} = 365 \times 364 \times \cdots \times 359 \times \frac{10!}{3!2!1!1!1!1!1!} \times \frac{1}{5!}$$

Mold : $\underline{AAA}\ \underline{BBB}\ \underline{CCC}\ D\ \underline{EE}\ \underline{FF}\ \underline{GG}\ H\ I\ J$

$$\log\left(\frac{20!}{3!\,3!\,3!\,2!\,2!\,2!\,2!\,1!\,1!\,1!\,1!} \times \frac{365 \times 364 \cdots \times 356}{1} \times \frac{1}{3!} \times \frac{1}{4!} \times \frac{1}{3!}\right)$$

$$(\log 20!) - (\log 3!) - (\log 3!) \cdots + \log 365 + \log 364 + \cdots + \log 356 - \log 3! - \log 4! - \log 3!$$

#people

people w/ birthday

all unique bdays

frequencies of frequencies

$$\log 5! = \log(4! \times 5)$$

$$= \log 4! + \log 5$$

$$\frac{3.8 \times 10^{2}}{10^{7}} \times \frac{2.7 \times 10^{5}}{}$$

$$.7 = \log 3.8 + \log 2.7$$

look up $\Rightarrow 10^{.7}$

Key Distribution

n users/nodes
any pair may need to communicate
via a shared secret key $\binom{n}{2}$ pairs.
$= \frac{n(n-1)}{2} \sim \frac{1}{2}n^2$

Key Distribution Center

KDC has 1 shared secret key with each of n users these are the Master keys.

Let's say user A wants to talk to user B.

1. User A $\longrightarrow$ KDS
   $ID_A \| ID_B \| N_1$ → nonce random #

2. KDS $\rightarrow$ User A
   $E(K_a, [K_s \| ID_A \| ID_B \| N_1]) \| E(K_b, [K_s \| ID_A])$
   (K_s: Session key)

3. User A $\rightarrow$ User B (a sends to b what KDC gave it)
   $E(K_b, [K_s \| ID_A])$

Just to prevent replay

4. User B $\rightarrow$ User A
   $E(K_s, N_2)$ → random #

5. User A $\rightarrow$ User B $E(K_s, f(N_2))$ ← some agreed upon function