

12/2/19 ①

① Birthday Paradox - Generalized Problem

② Key Distribution

Reg Birth Paradox

prob k diff birthdays out of k

$$\frac{365}{365} \times \frac{364}{365} \times \frac{363}{365} \times \dots \times \frac{365-k+1}{365} \leftarrow \begin{array}{l} \text{Sample} \\ \text{Space is} \\ 365^k \end{array}$$

for this problem

Sample Space = 365^k , $k = \text{total people}$
 $C_1 + C_2 + C_3 + \dots + C_n$

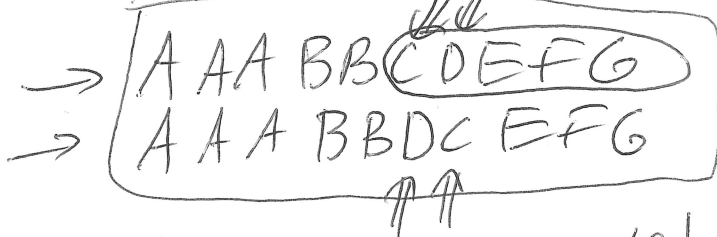
Goal: Count how many items in sample space are "successes"?

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

strings

A C D B E A B F A G \Rightarrow

$$\frac{10!}{3! 2! 1! 1! 1! 1! 1! 1!}$$



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

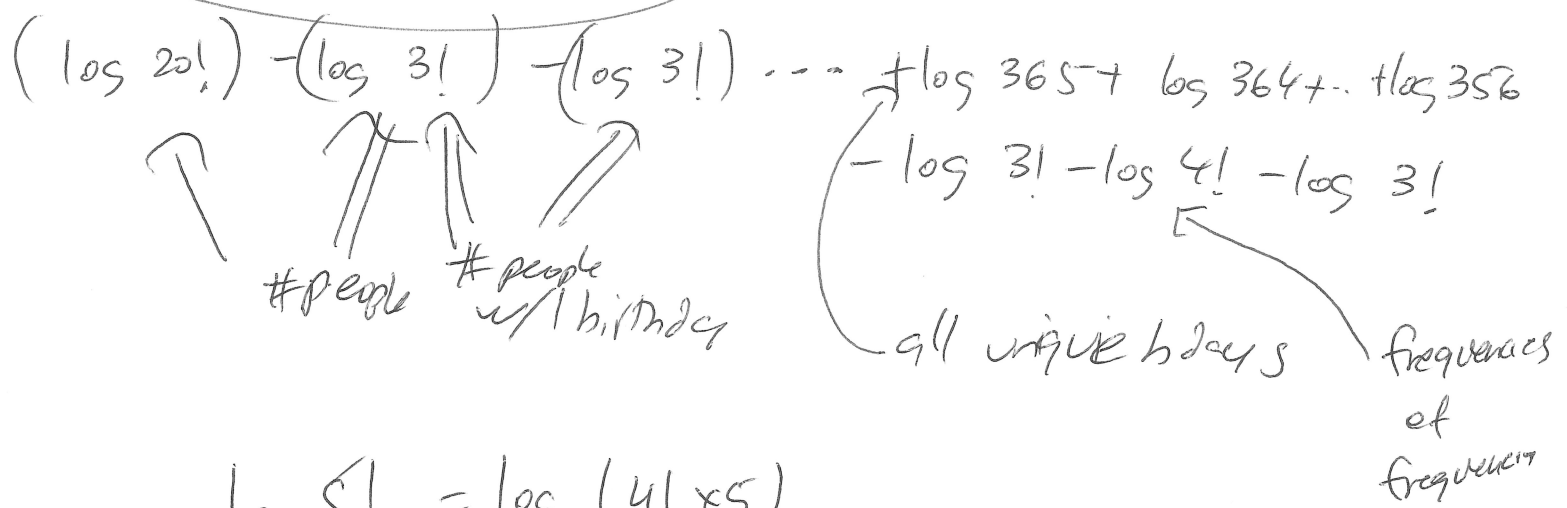
$$\# \text{Success} = 365 \times 364 \times \dots \times 359 \times \frac{10!}{3! 2! 1! 1! 1! 1! 1! 1!}$$

$$\times \frac{1}{5!}$$

Mold : AAA BBB CCC DD EEE FFF GG HIJ

$$\log \left(\frac{20!}{3! 3! 3! 2! 2! 2! 2! 1! 1! 1! 1!} \right)$$

$$\frac{365 \times 364 \dots \times 356}{1} \times \frac{1}{3!} \times \frac{1}{4!} \times \frac{1}{3!}$$



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

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

$$3.8 \times 10^2 \times 2.7 \times 10^5$$

$$.7 = \log 3.8 + \log 2.7 \quad 10^{-7}$$

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

Key Distribution

12/2/19 (3)

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 \rightarrow KDS

$ID_A \parallel ID_B \parallel N_1 \rightarrow$ nonce random #

2. KDS \rightarrow User A

$E(K_a, [K_s \parallel ID_A \parallel ID_B \parallel N_1]) \parallel E(K_b, [K_s \parallel ID_A])$

Session
key

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

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

5. User A \rightarrow User B $E(K_s, f(N_2))$

some agreed upon
function

Just
to
prevent
eaves
dropping