

11/22/19 (1)

Birthday Paradox $\longleftrightarrow$ Weak/Strong Collision Resistance

n people in room. What's probability all have diff birthdays?

$$\frac{365}{365} \times \frac{364}{365} \times \frac{363}{365} \times \frac{362}{365} \times \dots \times \frac{(365-n+1)}{365} < .5$$

min(n) st. $\nearrow$

$$\binom{23}{2} = \frac{23 \times 22}{2} = \text{253 pairs}$$

Weak: Given a fixed y , it hard to find an x such that $f(x)=y$.

Strong: Hard to find any pair x_1, x_2
 $x_1 \neq x_2$ and $f(x_1) = f(x_2)$.

$\rightarrow$ So if we have an n bit hash code on avg just have to generate $2^{n/2}$ messages before we get 2 that have the same hash code.