BIRTHDAY ATTACK

The birthday attack is a method to find collisions in a cryptographic hash function. It is based on the well known *"birthday paradox"* which says that if you have 23 people in a room then there is at least a 50% chance that two have the same birthday. Having the same birthday is the analogue of a *"collision"* in a hash function.

The Birthday Paradox

Assume we have 23 people in a room. We want to find the probability that two have the same birthday. The best way to do this is to find the probability that no two of these 23 people have the same birthday.

Assume we have 2 people in a room. There are 365^2 possible birthdays they can have. How many ways is it possible for them to have different birthdays? The first person's birthday can occur on 365 possible days. Then the second persons birthday can only occur on 364 possible days. So the probability that 2 people have different birthdays is

$$\frac{365 \cdot 364}{365^2} \approx 0.9972.$$

Assume we have 3 people in a room. There are 365^3 possible birthdays they can have. How many ways is it possible for them to have different birthdays? The first person's birthday can occur on 365 possible days. Then the second persons birthday can only occur on 364 possible days, while the third person's birthday can occur on 363 possible days. So the probability that 3 people have different birthdays is

$$\frac{365 \cdot 364 \cdot 363}{365^3} \approx 0.9912.$$

.
.
.

Assume we have 23 people in a room. There are 365^{23} possible birthdays they can have. How many ways is it possible for them to have different birthdays? The first person's birthday can occur on 365 possible days. Then the second persons birthday can only occur on 364 possible days, the third person's birthday can occur on 363 possible days, ..., while the 23^{rd} persons birthday can only occur on 343 possible days.
So the probability that 23 people have different birthdays is

$$\frac{365 \cdot 364 \cdot 363 \cdot 362 \quad \cdots \quad 343}{365^{23}} \approx 0.4927.$$