CSCI 357 - Cryptography
Ryan Kulyassa
HW #5 - Proof of Birthday Paradox

Prove the Birthday Paradox: Show that in a group of n people, the probability of at least two people sharing the same birthday exceeds 1/2 when n = 23. You can assume birthdays are uniformly distributed throughout the year (365 days).

To find this probability, we can first consider the complement probability, which in this case is the probability that 23 people do not share the same birthday. Therefore, we can calculate this as 365/365 * 364/365 * 363/365 … 343/365, or in other words $\frac{365!}{342!} \cdot \frac{1}{365^{23}}$. This is because as we count each person, there is one less possible birthday the next person can have, so the numerator decreases by one. Also, since the birthdays are uniformly distributed, they are all weighted the same. We do this 23 times, and the final product we get is 0.4927027657. Since this is the complement, we do 1-0.4927027657 = 0.507. Therefore, there is a **50.7%** probability that at least two people in a group of 23 share the same birthday, which is greater than ½.