CSCI 476 Computer Security

Exercise for Chapter 6.

(1) This **birthday paradox** problem has applications in DNS attack. The problem is based on this setting: in a room you have n people.

(1.1) How can you increase n so that there must be two people sharing the same birthday?

(1.2) The above is the worst-case analysis. Now what if you just want the probability that there are two people with the same birthday is at least 50%?