Cryptography Part II: Birthday Attack

Cryptographic Hardware for Embedded Systems

ECE 3894

Fall 2019

Assoc. Prof. Vincent John Mooney III
Georgia Institute of Technology

©Georgia Institute of Technology, 2018
How Many People Have Your Birthday?

• Assume that birthdays are randomly distributed throughout the year
  • E.g., 9 months after Aug. 29 is an equally likely birthday as any other day
  • Further assume Feb. 29 is excluded

• You walk into a room; how many people need to be in the room for there to be a 50% chance that one person has the same birthday as you?

• The chance that one person has the same birthday as you is 1/365

• The second person may have the same birthday as you or the first person
  ⇒ the increase in probability including the second person is not 1/365

• To get to approximately 50%, need to have 253 people in the room
What Are The Chances That Any Two People in a Room Have the Same Birthday?

• Two people: 1/365

  \[\Rightarrow\] a total chance of 3/365

  \[\Rightarrow\] a total chance of 6/365

• Clearly, growth of chances is more than linear (the growth is polynomial)

• Final result: with 23 people in the room, the chance that two people share the same birthday is approximately 50%
What Does the Birthday Attack Illustrate?

• The difference between the chances of randomly finding one particular secret, e.g., a match to a specific person’s birthday or the access code for a specific device

• Versus the chances of finding a collision, e.g., in a collection of devices two that have the same access code (key) or in a group of people any two who have the same birthday