Birthday and Replay Attacks

From Schneier

Attacks

- One-way functions can be used for message signatures/authenticators. *Note: The one-way function will be many-to-one*
- Matching a specific signature with a randomly generated message requires at worst 2^b attempts where b is the number of bits in a signature
- Example: choose one person of a group of 23, the probability that another person from the group will have the same birthday as this person is $1 - (364/365)^{22} \approx 0.06$ (Low)

From Schneier

Birthday Attack

- Problem `*birthday attack' on signature*: if it is easy to find two random messages that map to the same signature then a *birthday attack* is easy
- Example: the probability of 2 people having the same birthday in a group of 23 people is more than 0.5
- Difference from previous: did not pick a specific person's birthday to match