

Brute-forcing a hash function



CR - Collision Resistance

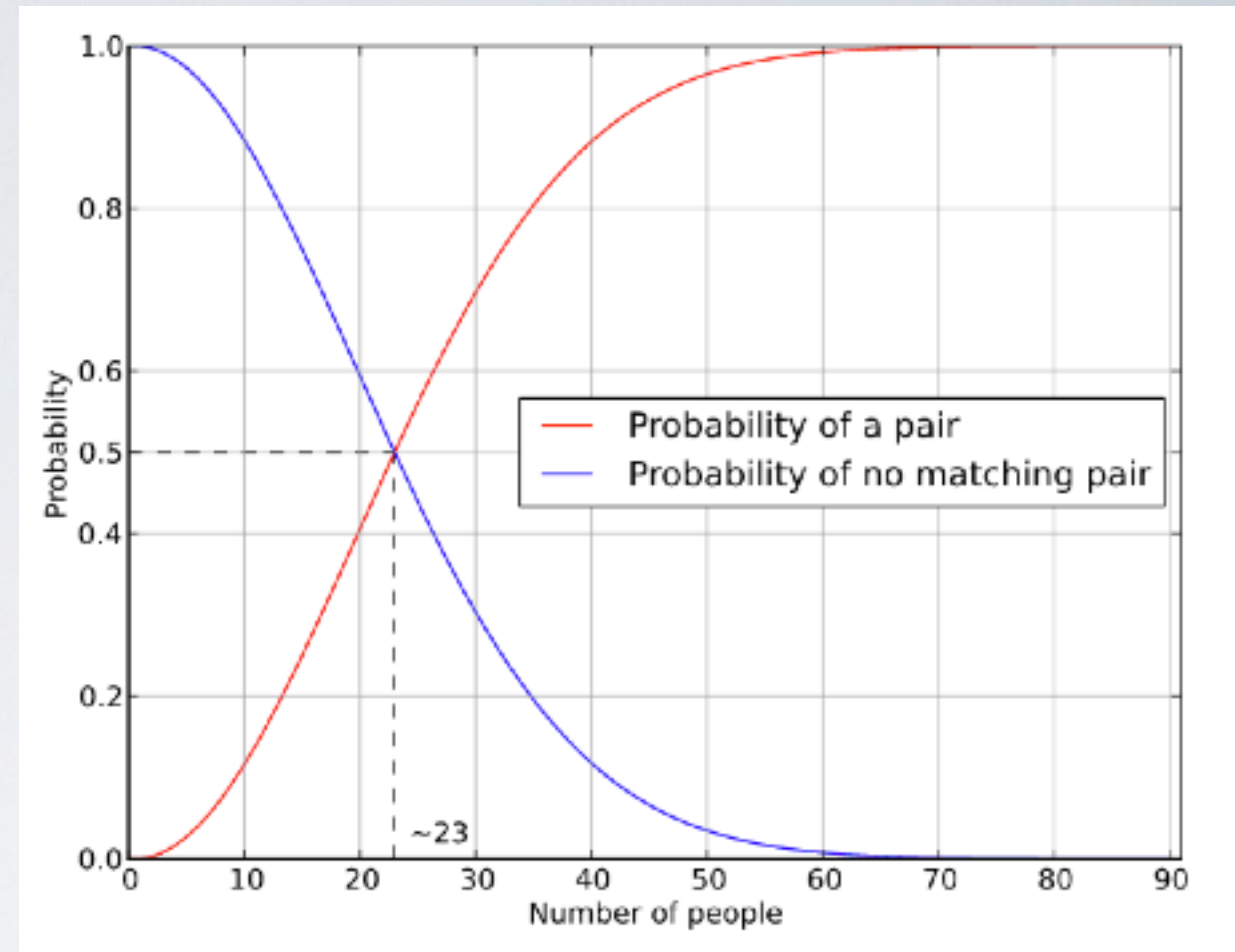
➡ given H , hard to find m and m' such that $H(m) = H(m') = x$

Given a hash function H of n bits output

- There are 2^n hashes
- Given a specific hash, an attacker will find the corresponding input in ~~2^{n-1} tries~~

Birthday Paradox

“There are 50% chance that 2 people have the same birthday in a room of 23 people”



N-bits security

- ➔ Given a hash function **H** of **n** bits output, a collision can be found in around **$2^{n/2}$** evaluations
e.g SHA-256 is 128 bits security