Brute-forcing a hash function

CR - Collision Resistance

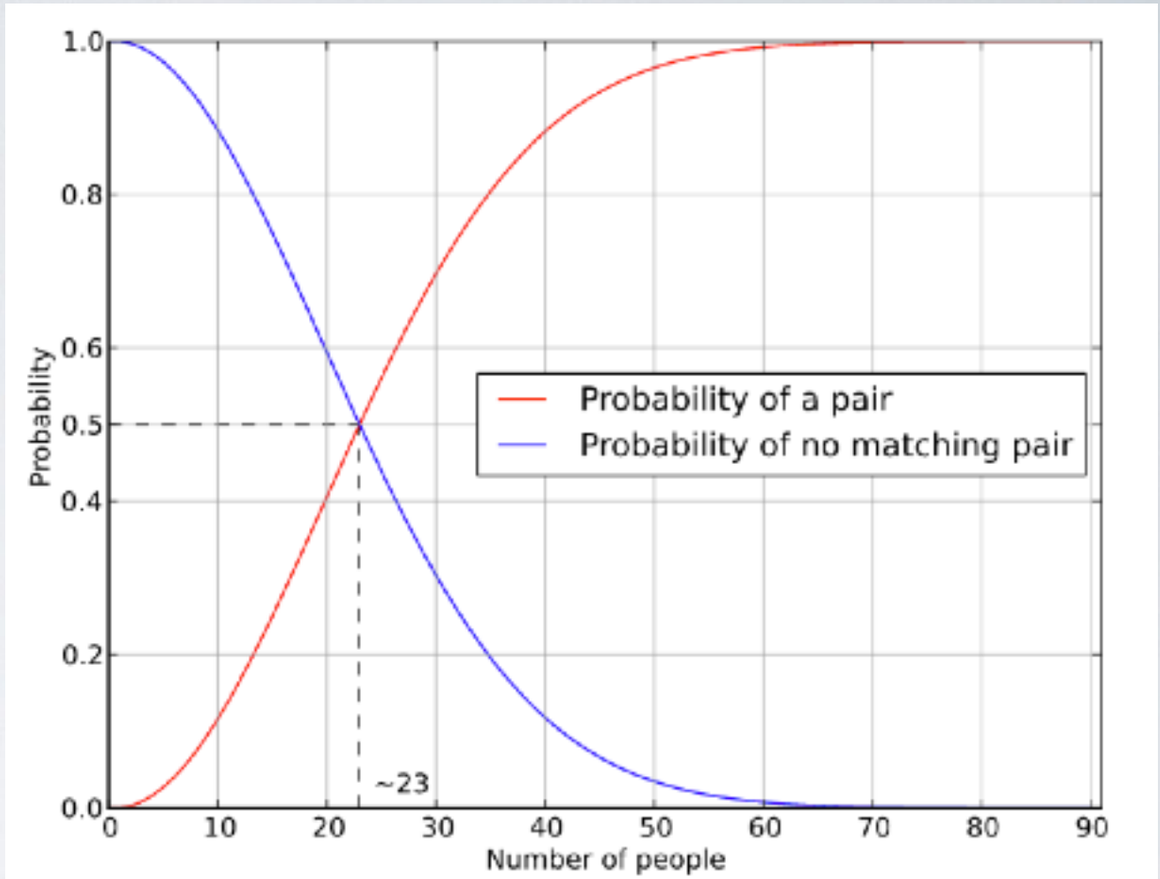
➡ given $\mathbf{H}$, hard to find $\mathbf{m}$ and $\mathbf{m'}$ such that $\mathbf{H(m) = H(m') = x}$

Given a hash function $\mathbf{H}$ of $\mathbf{n}$ bits output

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