Hash Functions

Many to one function?

fixed size output \ \g\ \ basic requirements

variable size input

\( f("HELLO HOW ARE YOU") \) - output fixed & b.5 multiple inputs can map to the same output.

Hash Table Operation

Store stuff in a table retrieve it quickly.

to store string "DOG" calculate \( f("DOG") = x \)

caller[2][3] = "DOG" or array[2][3].append("DOG").

Works well if there aren't lots of collisions.

Desirable Properties for Hash Func for Cryptos

1. Variable Input Size

2. Fixed Output Size

3. Fast

4. For any value \( y \), it should be computationally infeasible to find \( x \) such that \( f(x) = y \).

PRE-IMAGE RESISTANCE

5. For any \( x \), it should be hard to find \( x' \) such that \( f(x) = f(x') \), \( x' \neq x \).

SECOND PRE-IMAGE RESISTANCE

Computationally infeasible to find ANY \( x \) and \( x' \) s.t. \( x \neq x' \) and \( f(x) = f(x') \).

STRONG COLLISION RESISTANCE.
Use of Hash Functions

1. Passwords - one-way around
   If you just store $f(x)$ for each password $x$ and someone took common passwords and calculated the look up for matches.

2. Message Authentication