Hash Functions

Many to one function
fixed size output
variable size input
} basic requirements

f("HELLOHOWARE YOU") - output fixed @ b.t5
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
array[x] = "DOG" or array[x].append("DOG").
Works well if there aren't lots of "collisions".

Desirable Properties for Hash Func for Crypto

(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' ≠ x.
SECOND PREIMAGE RESISTANCE
(6) Computationally infeasible to find ANY, x and x' s.t. x ≠ x' and f(x) = f(x')
STRONG COLLISION RESISTANCE.

MORE + DIFFICULT TO OBTAIN

(7) Output should be pseudorandom - meet all randomness tests.

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 $f(x)$ looking for matches.

(2) Message Authentication