

Hash Functions

C2

Hash functions

Choosing a good hash function

Hash Functions

A hash function is a function $f(k)$ that maps a key, k , to a value, $f(k)$, within a prescribed range.

The key may be data of any size; the hash value is of fixed size.

A hash is deterministic. (For a given key, k , $f(k)$ will always be the same).

Choosing a Good Hash Function

A good hash for a given population, P , of keys, $k \in P$, will distribute $f(k)$ evenly within the prescribed range for the hash.

A *perfect hash* will give a unique $f(k)$ for each $k \in P$

For a *cryptographic hash*, it is infeasible to find k given $f(k)$, or to find two different keys that generate the same hash.