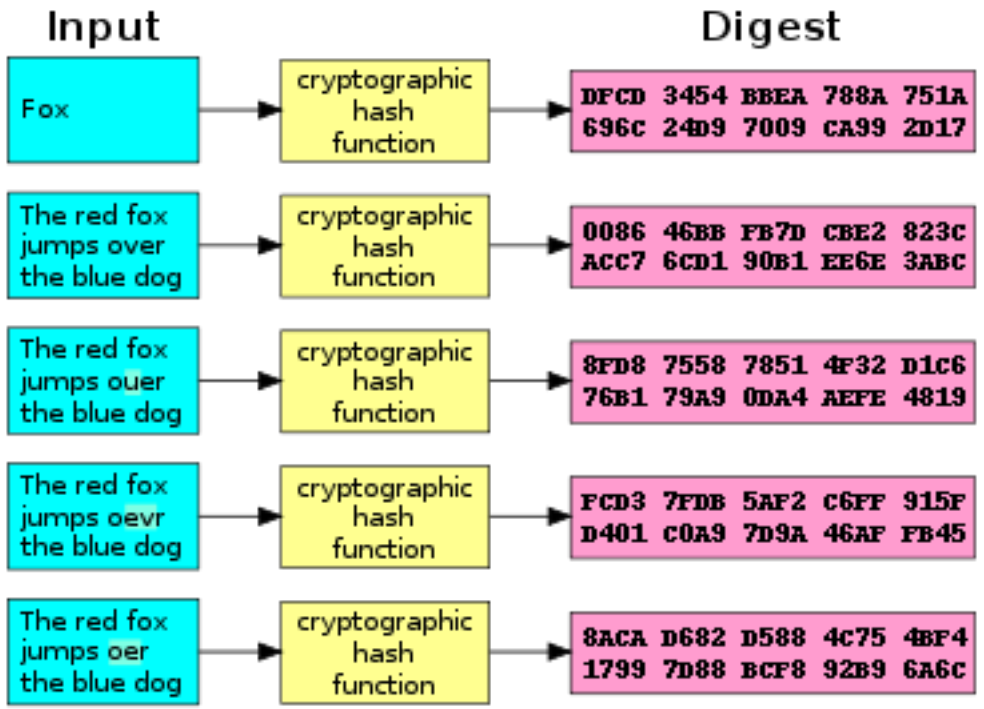
Hash Function

Hash Function

cryptographic hash function (CHF)

- a mathematical algorithm that maps data of arbitrary size to a bit array of a fixed size



https://en.wikipedia.org/wiki/File:Cryptographic_Hash_Function.svg

Hash Function Properties

- **Pre-Image Resistance**
  - hard to reverse a hash function
- **Second Pre-Image Resistance**
  - given an input and its hash, it should be hard to find a different input with the same hash
- **Collision Resistance**
  - it should be hard to find two different inputs of any length that result in the same hash

Design

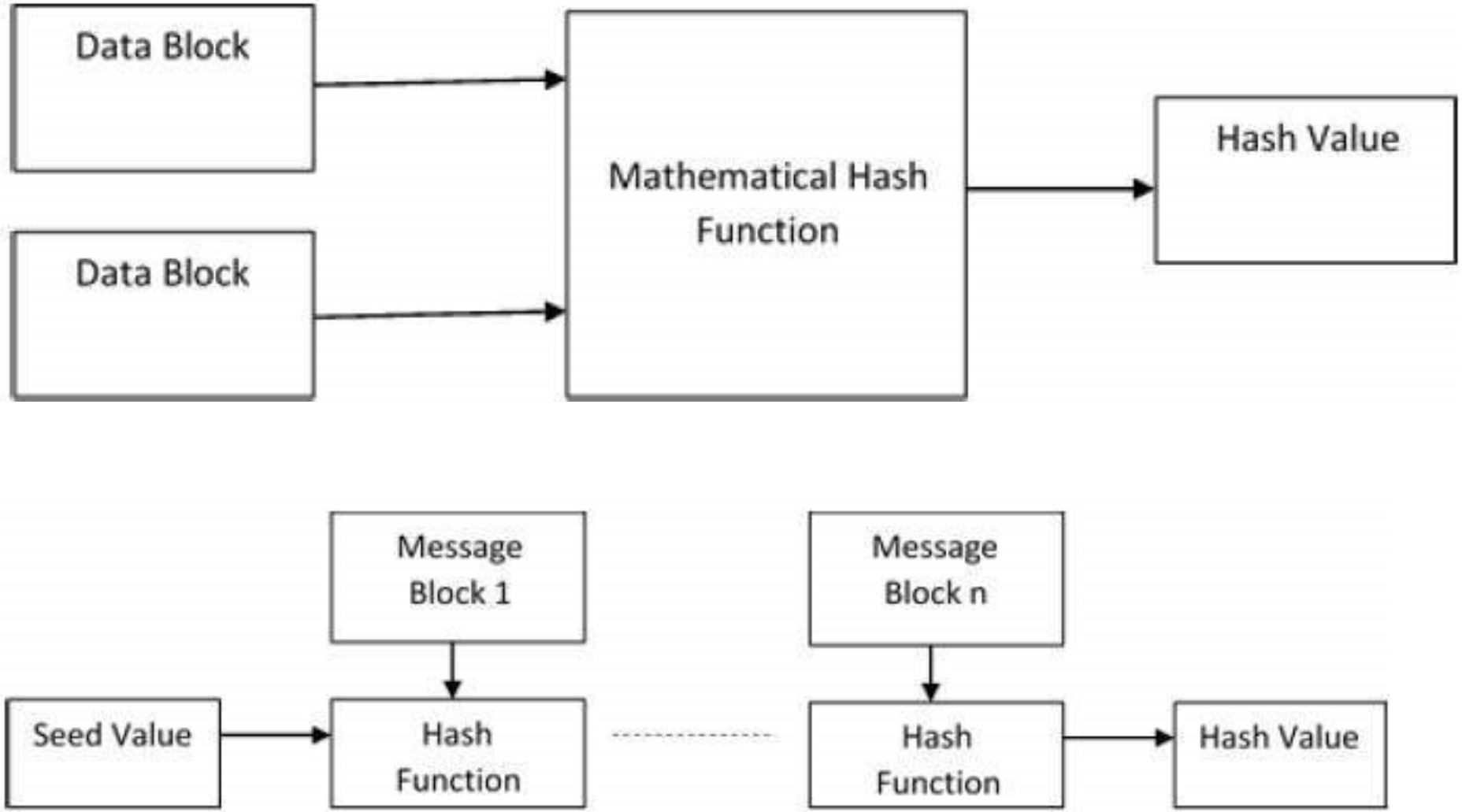


Figure: Schematic of hashing algorithm

Popular Hash Functions

- Message Digest (MD)
- Secure Hash Function (SHA)
- RIPEMD
- Whirlpool