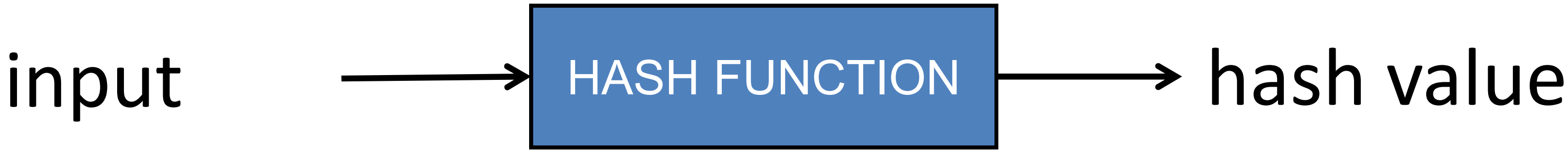

input → HASH FUNCTION → hash value

1. Easy (*for a computer*) to compute the hash for a string
2. Hard (*takes way too long*) to start with a hash value and construct a string that hashes to it
3. Impossible (*or near impossible*) to start with a string and find a different string that hashes to the same value -- ideal hash function will produce <u>unique</u> keys

Example of Salting "Jane Smith"

XOKZP**JANESMITH**

Increasing Security

Website Responsibilities

- Use Hashing
- Salt Passwords
- Secure the password file

User Responsibilities

- Defend against dictionary attacks
  - Use “unusual” passwords
- Defend against brute force/rainbow table attacks
  - Use long passwords
  - Use multiple character sets: a-z; A-Z; 0-9; punctuation.

Important Points

- Stealing the password file and checking passwords is called an ***offline attack***.
  - Something has already gone wrong, i.e. the site's password file has been stolen
  - Salting helps defend against this
  - Password stretching
- Attacks in which you repeatedly guess a password and try actually logging into the real site is called an ***online attack***
  - Throttling
  - Monitoring of system logs for unusual activity
- A useful defense against all attacks is to use multi-factor authentication
  - Something you know (a password)
  - Something you have/are
    - Smart card (have)
    - Fingerprint (identity -- are)
    - G-mail text message two factor authentication