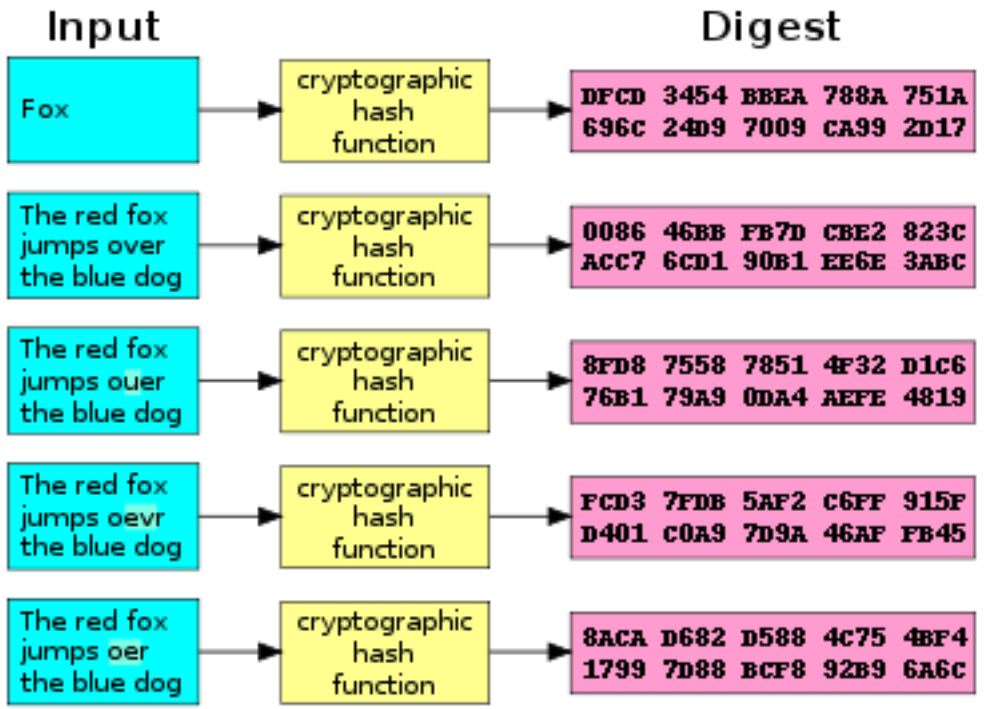
Hash Function

Hash Function

cryptographic hash function (CHF)

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

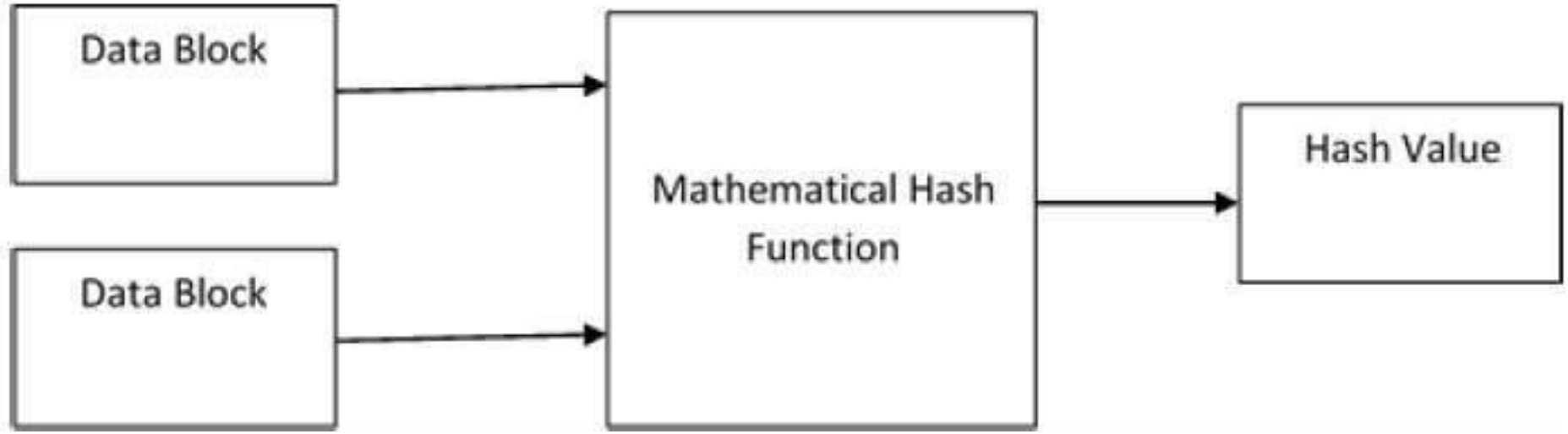


https://en.wikipedia.org/wiki/File:Cryptographic_Hash_Function.svg

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



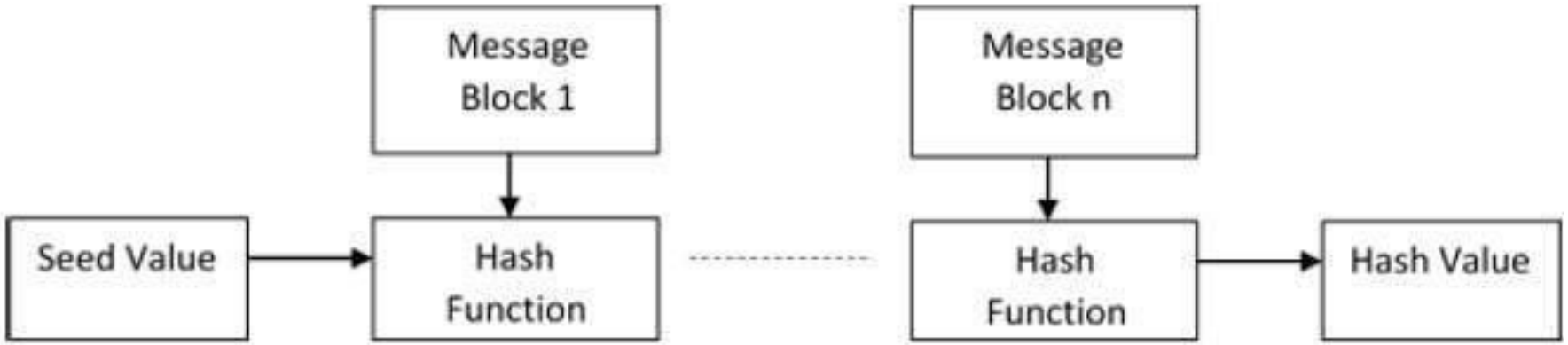


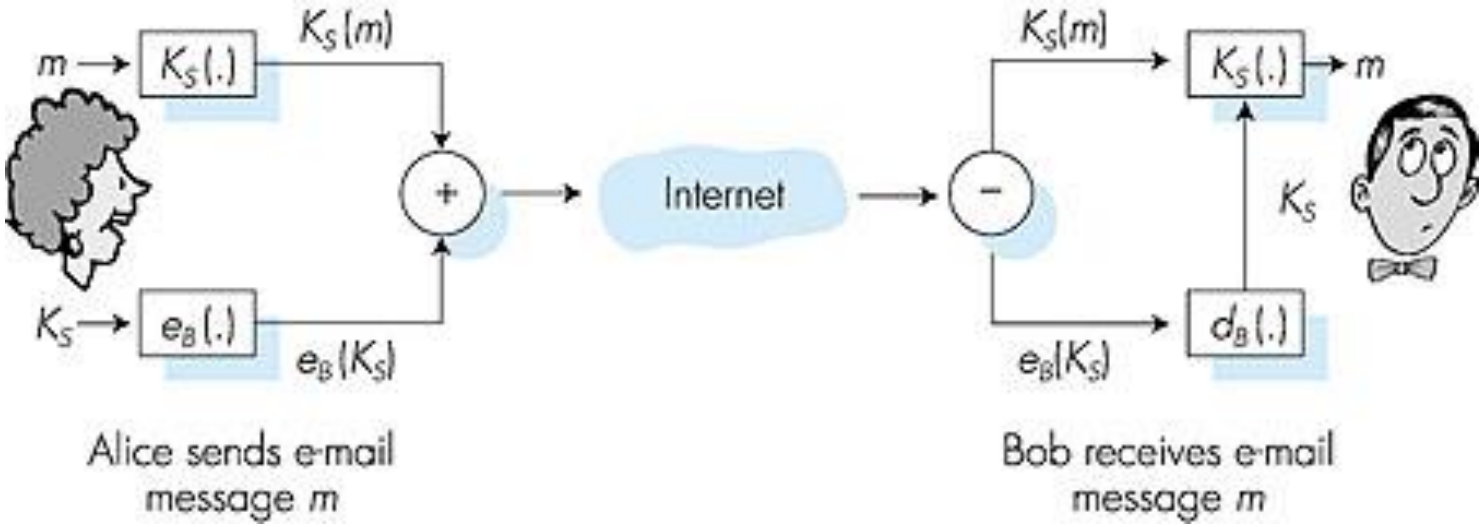
Figure: Schematic of hashing algorithm

Popular Hash Functions

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

Secure e-mail

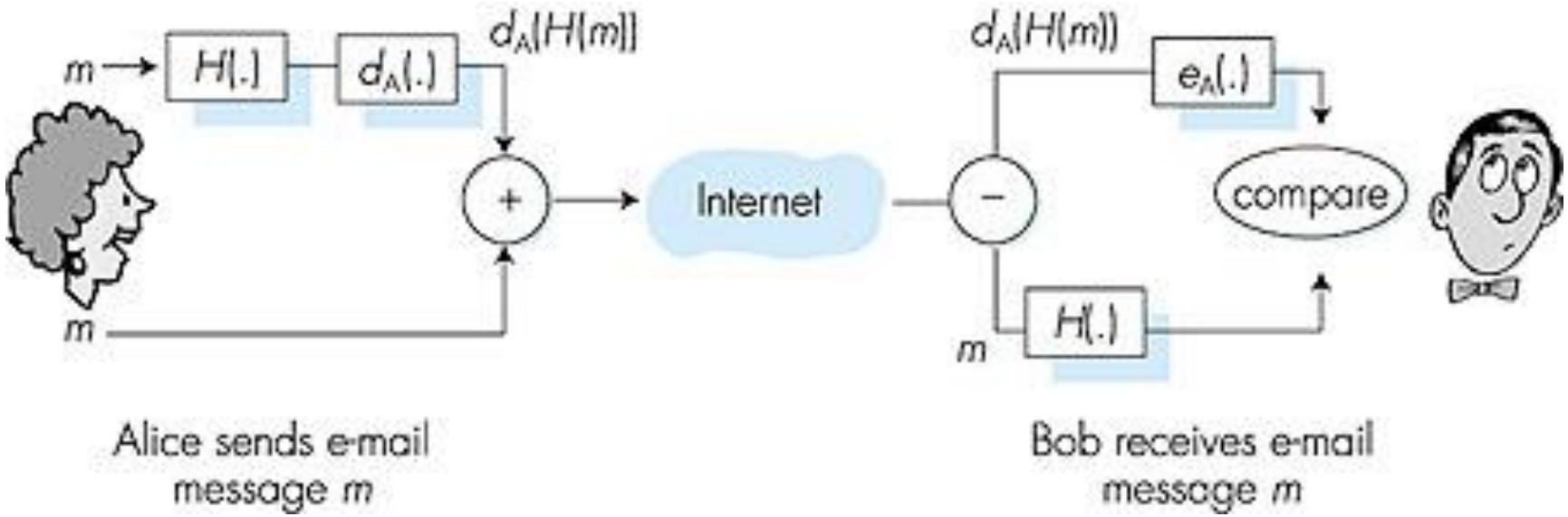
- Alice wants to send secret e-mail message, m, to Bob.



- generates random symmetric private key, K_S.
- encrypts message m with K_S
- also encrypts K_S with Bob's public key.
- sends both $K_S(m)$ and $e_B(K_S)$ to Bob.

Secure e-mail (continued)

• Alice wants to provide sender authentication message integrity.

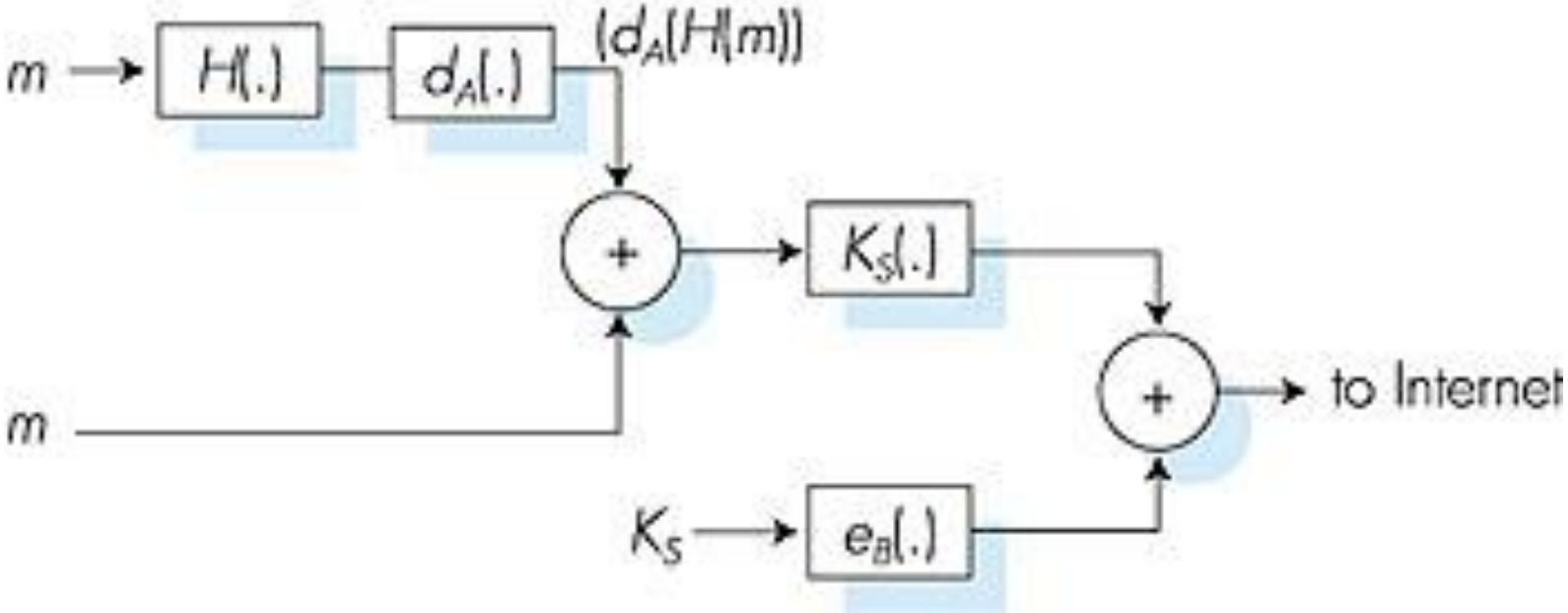


• Alice digitally signs message.
• sends both message (in the clear) and digital signature.

Secure e-mail (continued)

Alice wants to provide secrecy, sender authentication, message integrity.

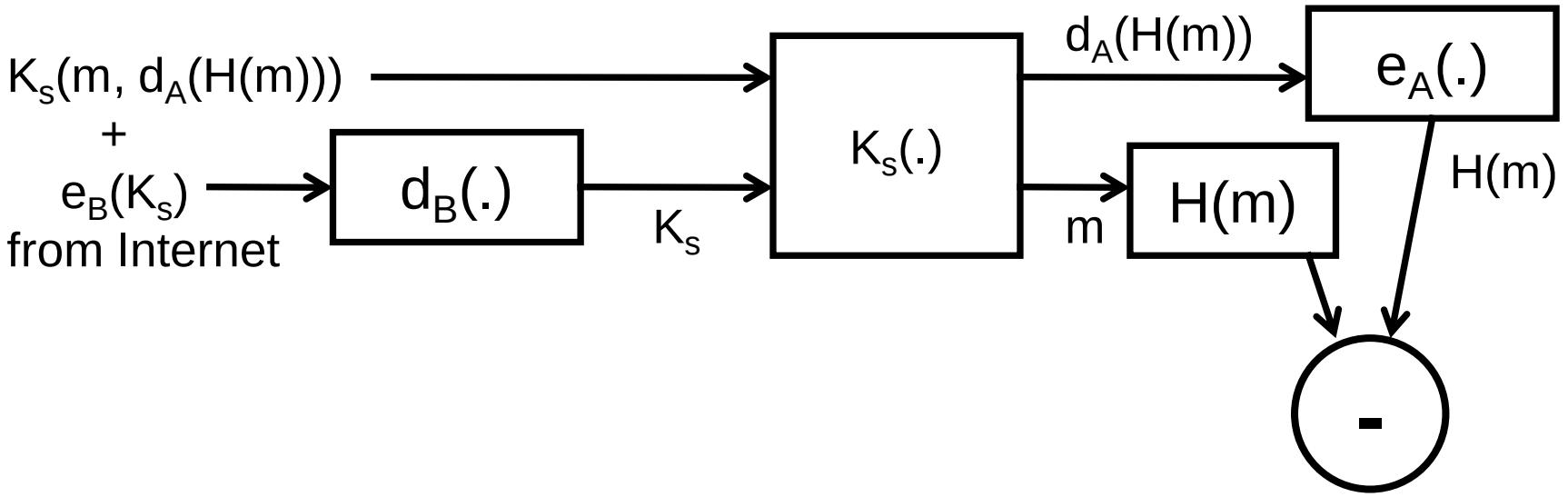
Alice hashes and encrypts the hash with her private key (dig. signature), adds the message and encrypts with a session key. Encrypts the session key with Bob's public key and sends both.



<u>Note:</u> Alice uses both her private key d_A, Bob's public key e_B.

Secure e-mail (continued)

Bob extracts session key with Bob's private key, extracts dig. sig. and message with session key and uses Alice's public key to extract hash from dig. sig. Hashes message and compares hashes.



Note: Bob uses Alice's public key e_A and Bob's private key d_B.