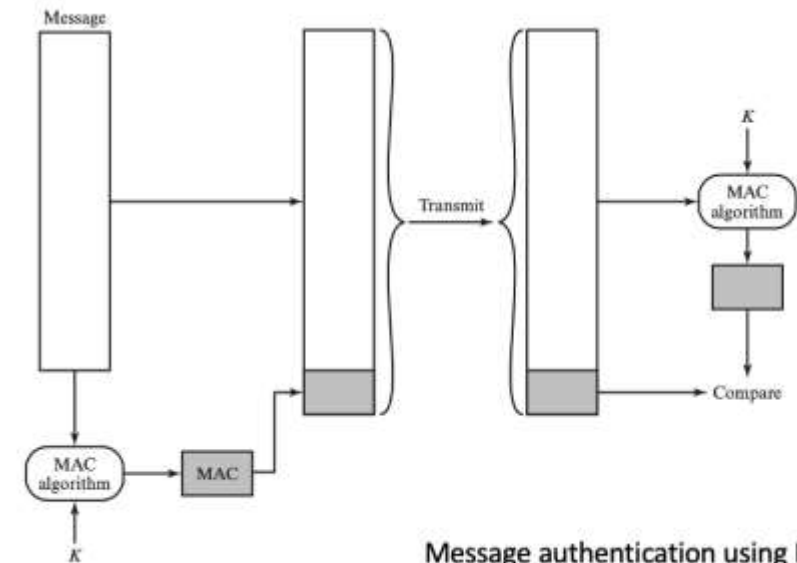


Lecture 15

Message Authentication

Message authentication

- message authentication is concerned with:
 - protecting the integrity of a message
 - validating identity of originator
 - non-repudiation of origin (dispute resolution)
- then three alternative functions used:
 - message encryption - symmetric
 - message authentication code (MAC)
 - digital signature



Message authentication using MAC

Message encryption

- Symmetric message encryption by itself also provides a measure of authentication
- if symmetric encryption is used then:
 - receiver knows sender must have created it
 - since only sender and receiver know key used
 - know content cannot be altered

Homework 1 questions

- Q1: Symmetric Block Cypher provides authentication and confidentiality
 - Ans: True

Message encryption

- if public-key encryption is used:
 - encryption provides no confidence of sender
 - since anyone potentially knows public-key
 - so, need to recognize corrupted messages
 - however, if
 - sender **signs** message using their private-key
 - then encrypts with recipients' public key
 - have both secrecy and authentication
 - but at cost of two public-key uses on message

Reasons to avoid encryption authentication

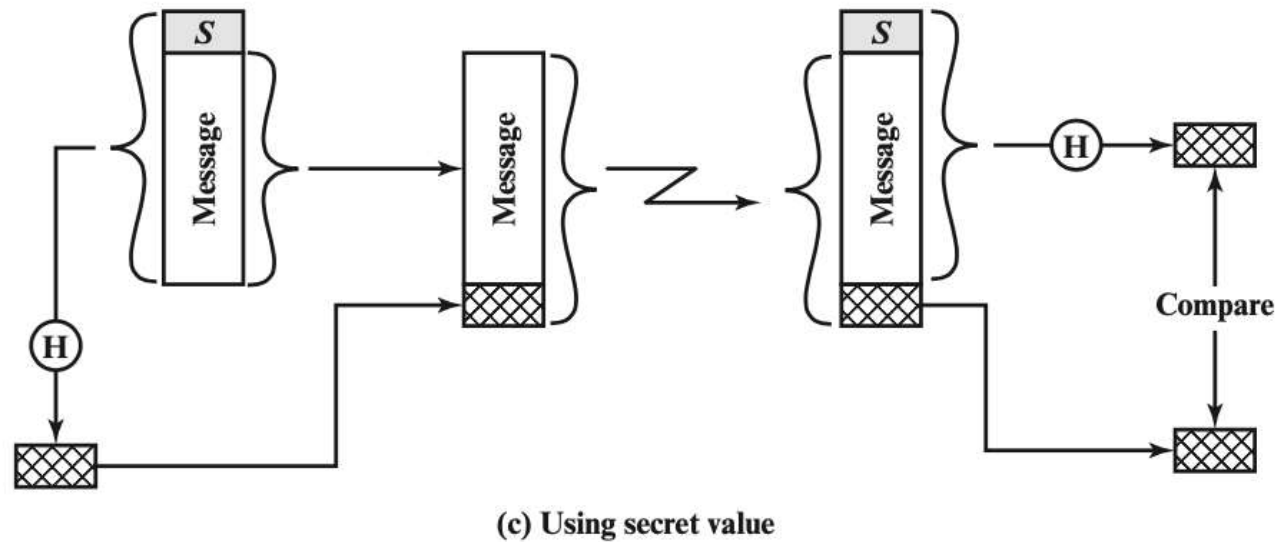
- Encryption software is quite slow
- Encryption hardware costs are nonnegligible
- Encryption hardware is optimized toward large data sizes
- An encryption algorithm may be protected by a patent

Hash Function

Hash functions

- Hash function: $h = H(M)$
 - M can be of any size
 - h is always of fixed size
 - Typically, $h \ll \text{size}(M)$

One use case - using hash function



- Initialization: A and B share a common secret, S_{AB}
- Message, M
- A calculates $MD_M = H(S_{AB} || M)$
- B recalculates MD'_M , and check
- $MD'_M = MD_M$

This scheme cannot provide authentication.