HASH FUNCTION, MAC, and HMAC
Lecture 5

COMPSCI 726
Network Defence and Countermeasures

Muhammad **Rizwan** Asghar

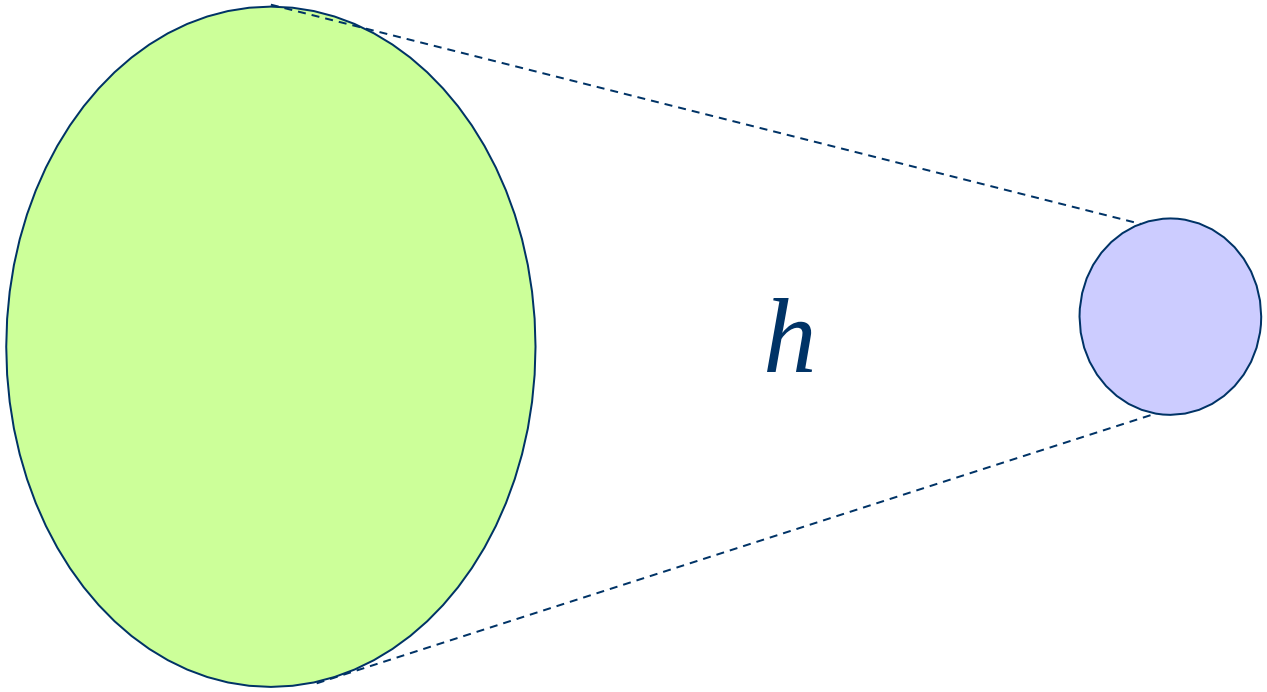
July 28, 2021

Source of some slides: **Stanford University**

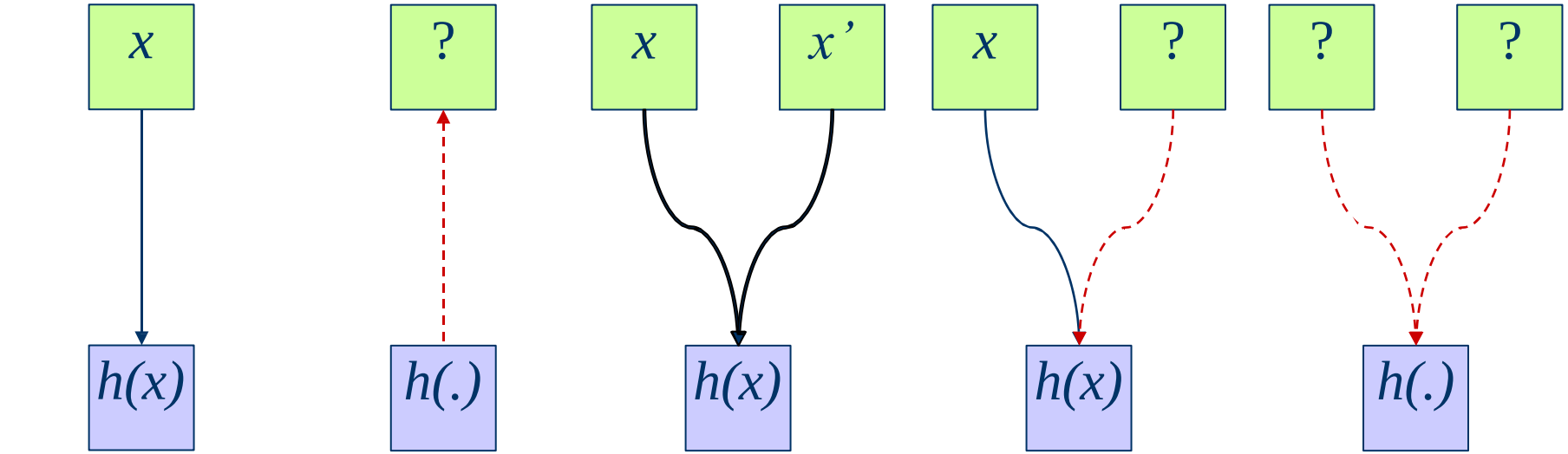
THE UNIVERSITY OF AUCKLAND
NEW ZEALAND

HASH FUNCTION

- Length-reducing function h
  - Maps an arbitrary string to a fixed-length string
- Publicly known
- Also known as cryptographic checksum or message digest



HASH PROPERTIES



Ease of computation

Pre-image resistance

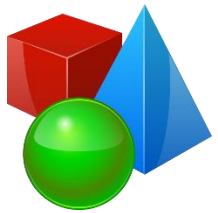
Collision

2nd pre-image resistance

Collision resistance

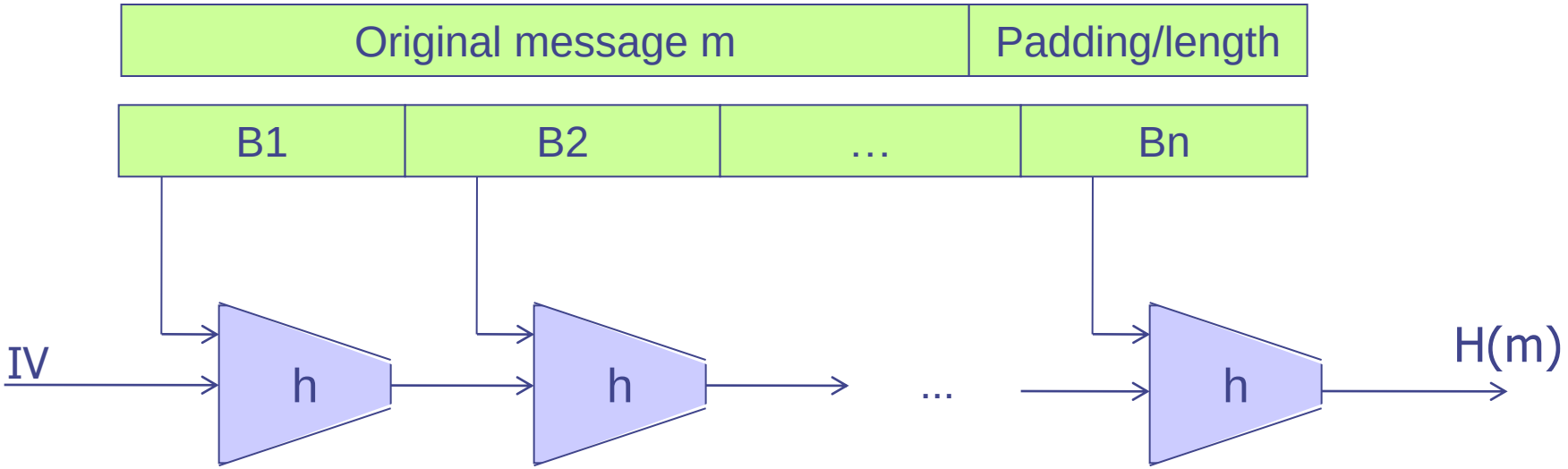
- Collision resistance implies 2nd pre-image resistance

COMMONLY USED HASH FUNCTIONS



- **MD** (Message Digest)
  - MD5
    - Max message < 2^{64}
    - Output: 128-bit
- **SHA** (Secure Hash Algorithm)
  - SHA-1
    - Max message < 2^{64}
    - Output: 160-bit
  - SHA-2
    - Max message < 2^{128}
    - Max output: 512-bit
  - SHA-3
    - Max message: Unlimited
    - Max output: 512-bit

SHA-512: MERKLE-DAMGARD SCHEME



- Augmented message: multiple of 1024-bit blocks
- h(., Bi) is a compression function
- Theorem: If h is collision resistant then so is H

HASH APPLICATIONS

- Detect changes to messages/files (integrity)
- Digital signatures
  - Sign hash of message instead of entire message
- Psudorandom function (PRF)
  - Generate session key, nonce (Number Only Once)
  - Produce key from password
  - Derive keys from master key
- Create one-way password file
  - Store hash of password
    - Salt to harden pre-computed dictionary attacks
- Viruses and intrusion detection
- Auctions: To bid B, send *h*(B) and reveal B later

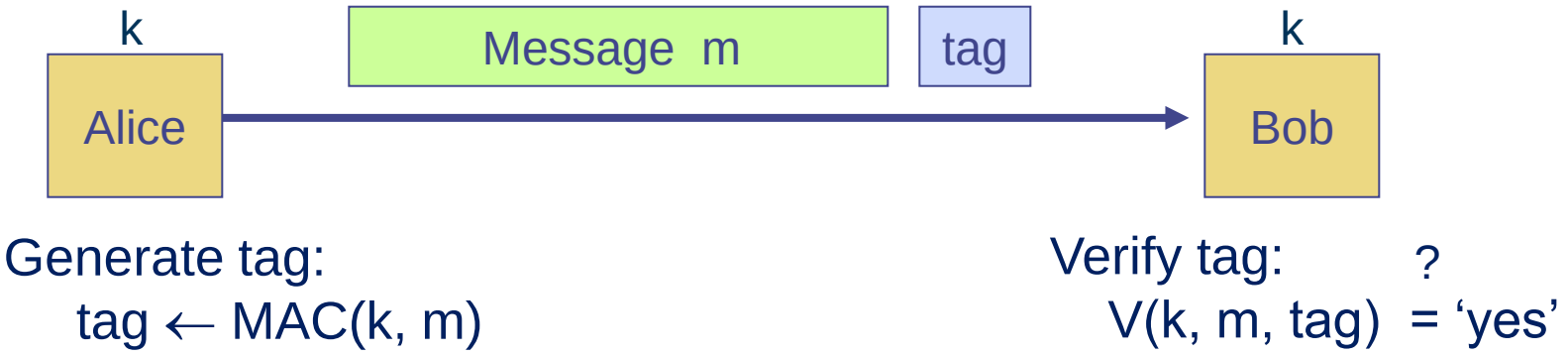
HASH VS. ENCRYPTION

- Hashing is a one-way
  - No unhashing
- Publicly known and there is no key used
- Efficient
- Deterministic (compared)
  - H(m) == H(m')
  - Of course, hashes with salts are not!
    - H(m || s1) and H(m || s2)

- Encryption is not one-way
  - Decryption renders the original message
- Publicly known algorithms but the key is kept secret
- Slower
- May or may not be deterministic (compared)
  - Randomised encryption
    - Enc(k, t1 || m) and Enc(k, t2 || m)

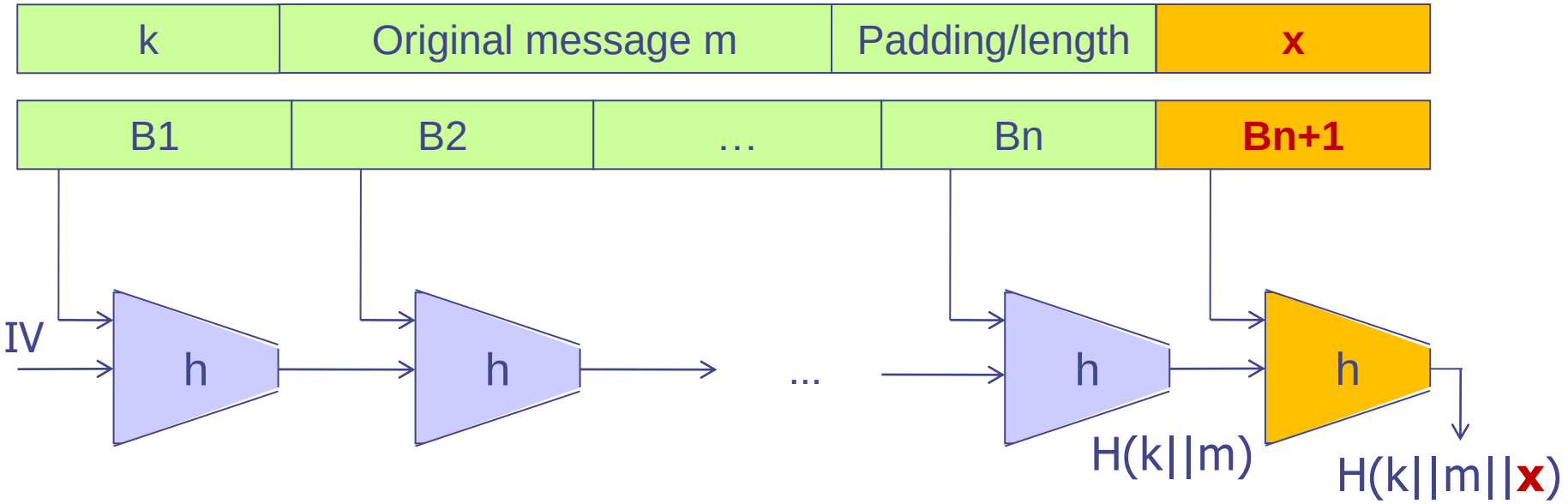
MESSAGE AUTHENTICATION CODE (MAC)

- Like a hash function, but it uses a key!
- Appended to the original message
- Receiver performs same computation on the message and checks if it matches the MAC
- It provides assurance that the message is unaltered and comes from the sender



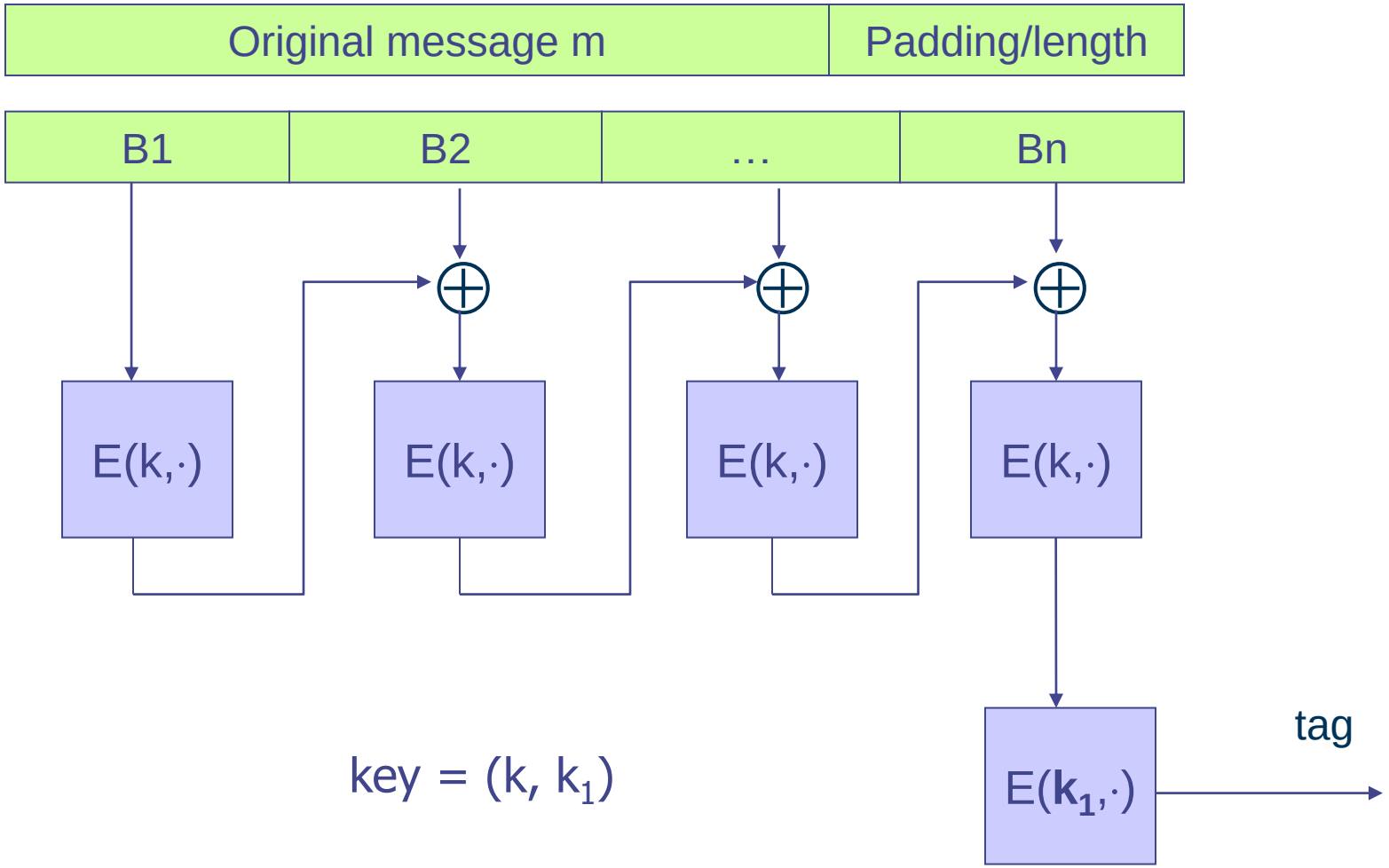
MAC CONSTRUCTION: MERKLE-DAMGARD SCHEME

- MAC(k, m) = H(k || m)



- Issue: Length extension attack!

MAC CONSTRUCTION: RAW CBC



MAC APPLICATIONS

- Integrity of a message or file
- Validating identity of a message sender (authentication)

HASH VS. MAC

- Publicly known and no key
- A hash value
- Efficient
- Message integrity
- Anyone can generate it

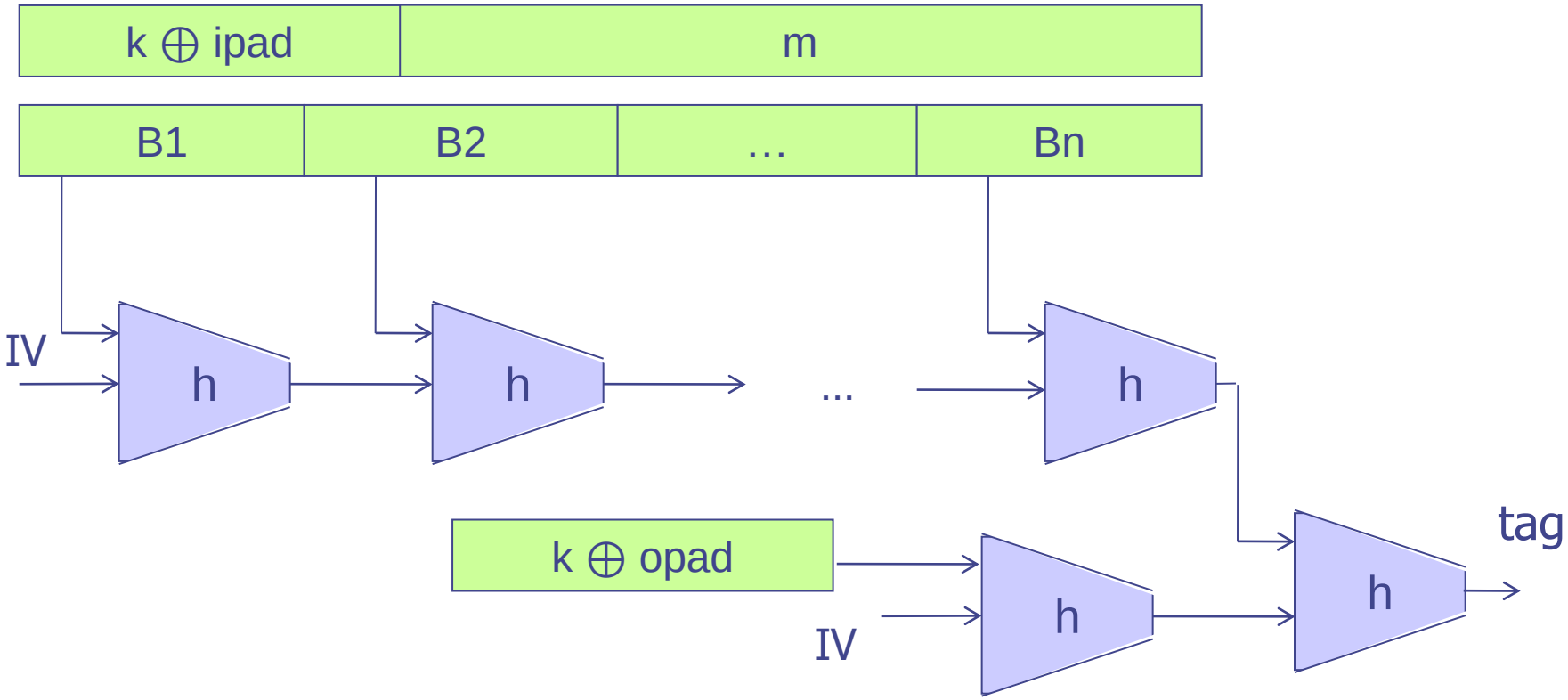
- Publicly known, but the key is kept secret
- A keyed hash value
- Slower
- Message integrity and authentication
- Only an authorised user can generate it

HASH-BASED MAC (HMAC)

- Evolved from weakness in MAC
- A specific construction of calculating a MAC involving a secret key
- Uses and handles the key in a simple way
- Less effected by collision than underlying hash algorithm
- More secure

HMAC CONSTRUCTION: MERKLE-DAMGARD SCHEME

- HMAC(k, m) = H(k ⊕ opad || H(k ⊕ ipad || m))

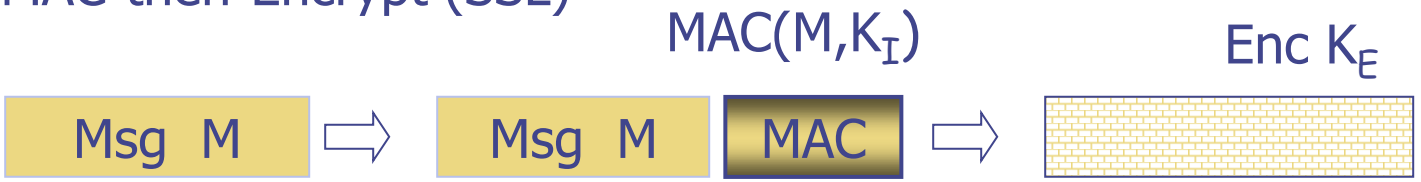


- Theorem: If h is a PRF then HMAC is a PRF

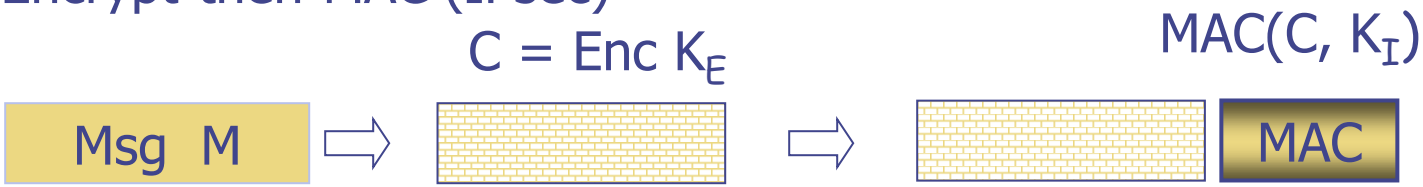
AUTHENTICATED ENCRYPTION

Encryption key K_E MAC key = K_I

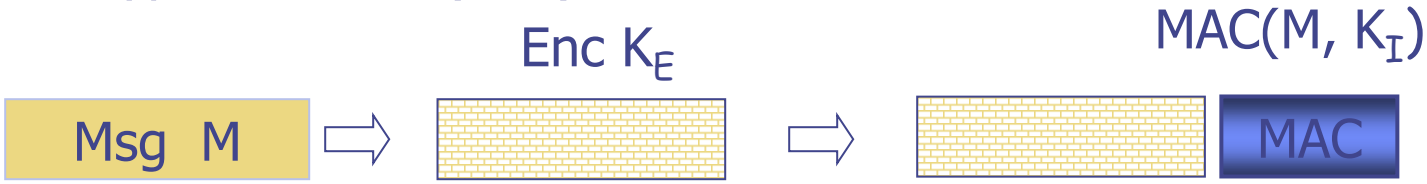
Option 1: MAC-then-Encrypt (SSL)



Option 2: Encrypt-then-MAC (IPsec)



Option 3: Encrypt-and-MAC (SSH)



SUMMARY

- Hash is a one-way function, which is easy to compute but difficult to invert
- MAC offers both data integrity and authentication
- Authenticated encryption combines both encryption and MAC

RESOURCES

- Read Chapter 3 of
  Network Security Essentials – Applications and Standards
  Fourth Edition
  William Stallings
  Prentice Hall
  ISBN 0-13-706792-5

Questions?

Thanks for your attention!