

# Lecture 6'

**Cryptographic Hash Functions  
and Message Digests  
(last few slides from  
02/01/07)**

1

What are hash functions  
good for?

2

## Message Authentication Using a Hash Function

Use symmetric encryption such as AES or 3-DES

- Generate  $H(M)$  of same size as  $E()$  block
- Use  $E_k(H(M))$  as the MAC
- Alice sends  $E_k(H(M))$ ,  $M$
- Bob receives  $C, M'$  decrypts  $C$  with  $k$ , hashes  $M'$  and compares to  $H(M')$

$$H(D_k(C)) \stackrel{?}{=} H(M')$$

**Collision  $\rightarrow$  MAC forgery!**

3

## Using Hash for Authentication

- Alice to Bob: random challenge  $r_A$
- Bob to Alice:  $H(K_{AB} || r_A)$
- Bob to Alice: random challenge  $r_B$
- Alice to Bob:  $H(K_{AB} || r_B)$
- Only need to compare  $H()$  results

4

## Using Hash to Compute MAC: integrity

- **Cannot just compute and append  $H(m)$**
- **Need "Keyed Hash":**
  - ❖ **Prefix:**
    - **MAC:**  $H(K_{AB} || m)$ , almost works, but...
    - **Allows concatenation with arbitrary message:**  
 $H(K_{AB} || m || m')$
  - ❖ **Suffix:**
    - **MAC:**  $H(m || K_{AB})$ , works better, but what if  $m'$  is found such that  $H(m) = H(m')$ ?
  - ❖ **HMAC:**
    - $H(K_{AB} || H(K_{AB} || m))$

5

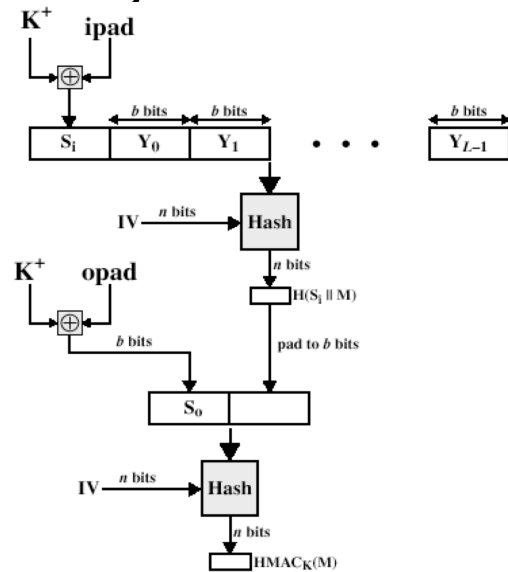
## Hash Function MAC (HMAC)

- **Main Idea:** Use a MAC derived from any cryptographic hash function
  - ❖ Note that hash functions do not use a key, and therefore cannot serve directly as a MAC
- **Motivations for HMAC:**
  - ❖ Cryptographic hash functions execute faster in software than encryption algorithms such as DES
  - ❖ No need for the reverseability of encryption
  - ❖ No export restrictions from the US (was important in the past)
- **Status:** designated as mandatory for IP security
  - ❖ Also used in Transport Layer Security (TLS), which will replace SSL, and in SET

6

# HMAC Algorithm

- Compute  $H_1 = H()$  of the concatenation of  $M$  and  $K_1$
- To prevent an "additional block" attack, compute again  $H_2 = H()$  of the concatenation of  $H_1$  and  $K_2$
- $K_1$  and  $K_2$  each use half the bits of  $K$
- Notation:
  - ❖  $K^+ = K$  padded with 0's
  - ❖  $\text{ipad} = 00110110 \times b/8$
  - ❖  $\text{opad} = 01011100 \times b/8$
- Execution:
  - ❖ Same as  $H(M)$ , plus 2 blocks



7

## Using Hash to Encrypt : confidentiality

- (Almost) One-time pad: similar to OFB
  - ❖ compute bit streams using  $H()$ ,  $K$ , and IV
    - $b_1 = H(K_{AB} || IV), \dots, b_i = H(K_{AB} || b_{i-1}), \dots$
    - $c_i = p_i \oplus b_1, \dots, c_i = p_i \oplus b_i, \dots$
- Or, mix in the plaintext
  - ❖ similar to cipher feedback mode (CFB)
    - $b_1 = H(K_{AB} || IV), \dots, b_i = H(K_{AB} || c_{i-1}), \dots$
    - $c_i = p_i \oplus b_1, \dots, c_i = p_i \oplus b_i, \dots$

8