Introduction to Cryptography CS 355

Lecture 29

HMAC and CBC-MAC

Lecture Outline

- HMAC
- CBC-MAC
- Combining data integrity with encryption

HMAC Goals

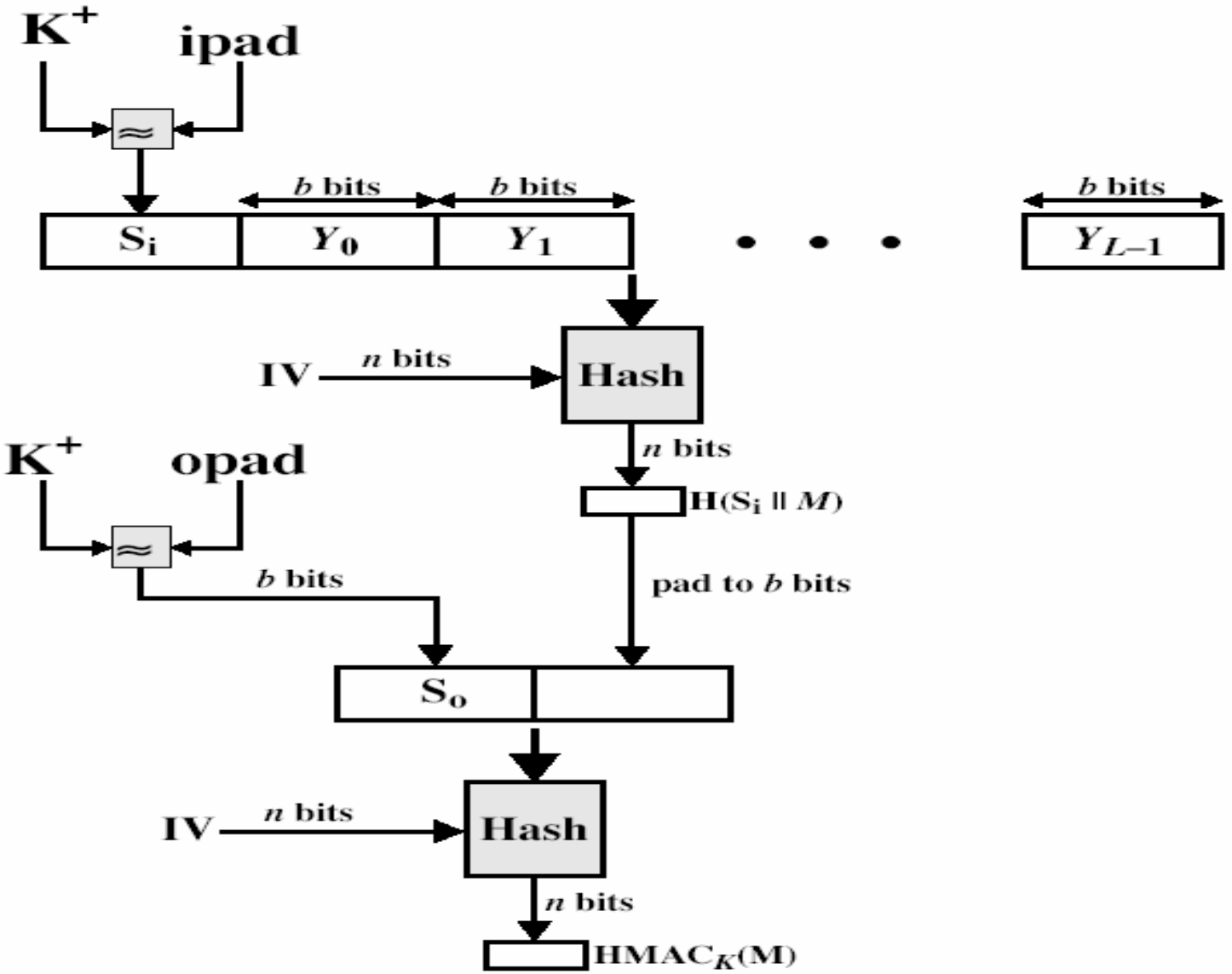
- Use available hash functions without modification.
- Preserve the original performance of the hash function without incurring a significant degradation.
- Use and handle keys in a simple way.
- Allow easy replacement of the underlying hash function in the event that faster or more secure hash functions are later available.
- Have a well-understood cryptographic analysis of the strength of the authentication mechanism based on reasonable assumptions on the underlying hash function.

HMAC

$$HMAC_K = Hash[(K^+ \oplus opad) \,||\, Hash[(K^+ \oplus ipad)||M)]]$$

- K^+ is the key padded out to input block size of the hash function and opad, ipad are specified padding constants
- Key size: $L/2 < K < L$
- MAC size: at least L/2, where L is the hash output

HMAC Overview



HMAC Security

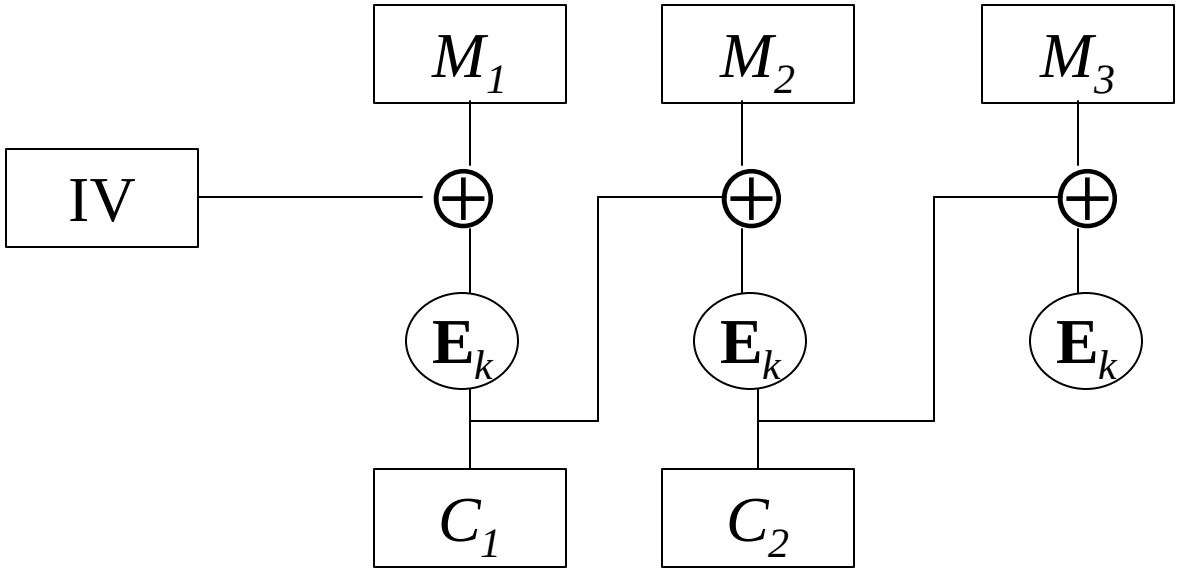
- Security of HMAC relates to that of the underlying hash algorithm
- If used with a secure hash functions (s.t. SHA1) and according to the specification (key size, and use correct output), no known practical attacks against HMAC
- In general, HMAC can be attacked as follows:
  - brute force on the key space
  - attacks on the hash function itself
    - birthday attack, although the use of key makes this attack more difficult
    - attacks against the compression function

CBC-MAC

- Given a block cipher **E** with block size m
- Given message $M = M_1 \,||\, M_2 \,||\, \ldots \,||\, M_n$
- MAC of M is $\mathbf{E}_k(M)$
  - $z_0 = IV = 0^m$
  - $z_i = \mathbf{E}_k(z_{i-1} \oplus M_i)$ for $1 \le i \le n$
  - $MAC = z_n$
- Random IV is needed in CBC encryption to prevent codebook attack on first block, not needed here.

Encryption Modes: CBC

- Cipher Block Chaining (CBC): next input depends of previous output
  - Plaintext is *M1*, *M2*, *M3*, *M4*,
  - Ciphertext is: $C_1 = \text{IV} \oplus \mathbf{E}_k(M_1)$ $C_2 = C_1 \oplus \mathbf{E}_k(M_2)$ $C_3 = C_2 \oplus \mathbf{E}_k(M_3)$ $C_4 = C_3 \oplus \mathbf{E}_k(M_4)$



Security of CBC-MAC

- Secure for messages of a fixed number of blocks assuming the block cipher is PRP
- Not secure with variable lengths

Data Integrity Combined with Encryption

- Encryption alone does not guarantee data integrity
  - possible attacks: reordering ECB blocks,
- Approach 1: Combining encryption with hash
  - $C=E_K[x \,||\, h(x)]$
  - breaking encryption also compromises integrity
  - may be vulnerable to known-plaintext attack

MAC with Encryption

- $C=E_K[x \,||\, h_{K'}(x)]$
  - separate keys used for encryption & for MAC
  - the algorithms E and h should be independent
  - precludes exhaustive key search on MAC key
- Alternative 1: $C=E_K[x], h_{K'}(E_K[x])$
  - allows message authentication without knowing x or K
  - authenticates only the ciphertext
- Alterative 2: $E_K[x],h_{K'}(x)$
  - requires $h_{K'}(x)$ does not leak information about x

Coming Attractions …

- Digital Signatures