Fundamentals of Information & Network Security
ECE 471/571

Lecture #18: Hash and Message Authentication Code

Instructor: Ming Li
Dept of Electrical and Computer Engineering
University of Arizona

Message Authentication Code

- MD(m) ?
- MD(K_{AB}|m): only the one who knows the secret can compute/verify
- Problem?

The Problem with keyed hash *h(Key|m)*

- A feature of message digest algorithms
  - In order to compute the message digest through chunk *n*, all that you need to know is the message digest through chunk *n-1*, plus the chuck *n* of the padded message.
- An Attack
  - Someone gets m, and digest(Key|m)
  - He first pads m according the used hash function, and then adds another message M at the end. The result is m|pad|M.
  - digest(Key|m|pad |M) can be calculated from digest(Key|m), which is the intermediate digest.

Solutions

- Use h(m|Key)
- HMAC

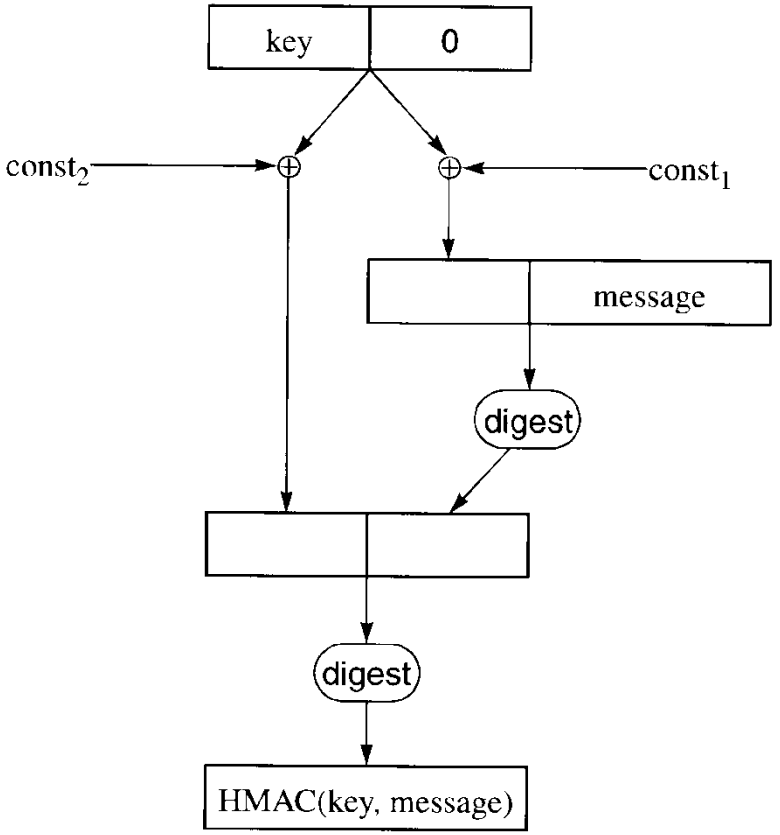


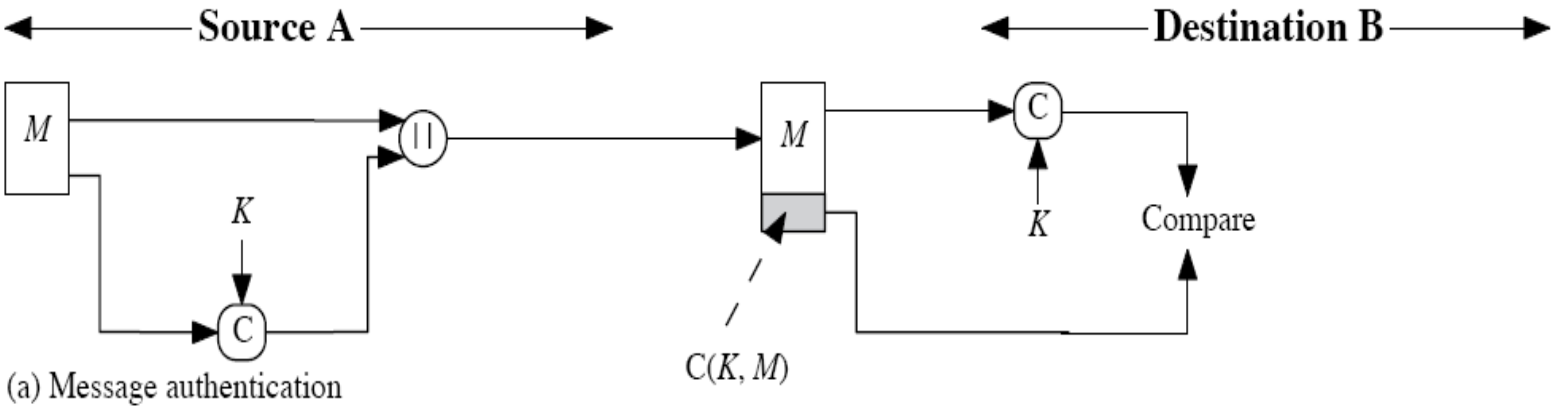
Figure 5-10. HMAC

$$\mathrm{HMAC}_K(x) = \mathrm{SHA\text{-}1}((K \oplus opad) \,||\, \mathrm{SHA\text{-}1}((K \oplus ipad) \,||\, x)).$$

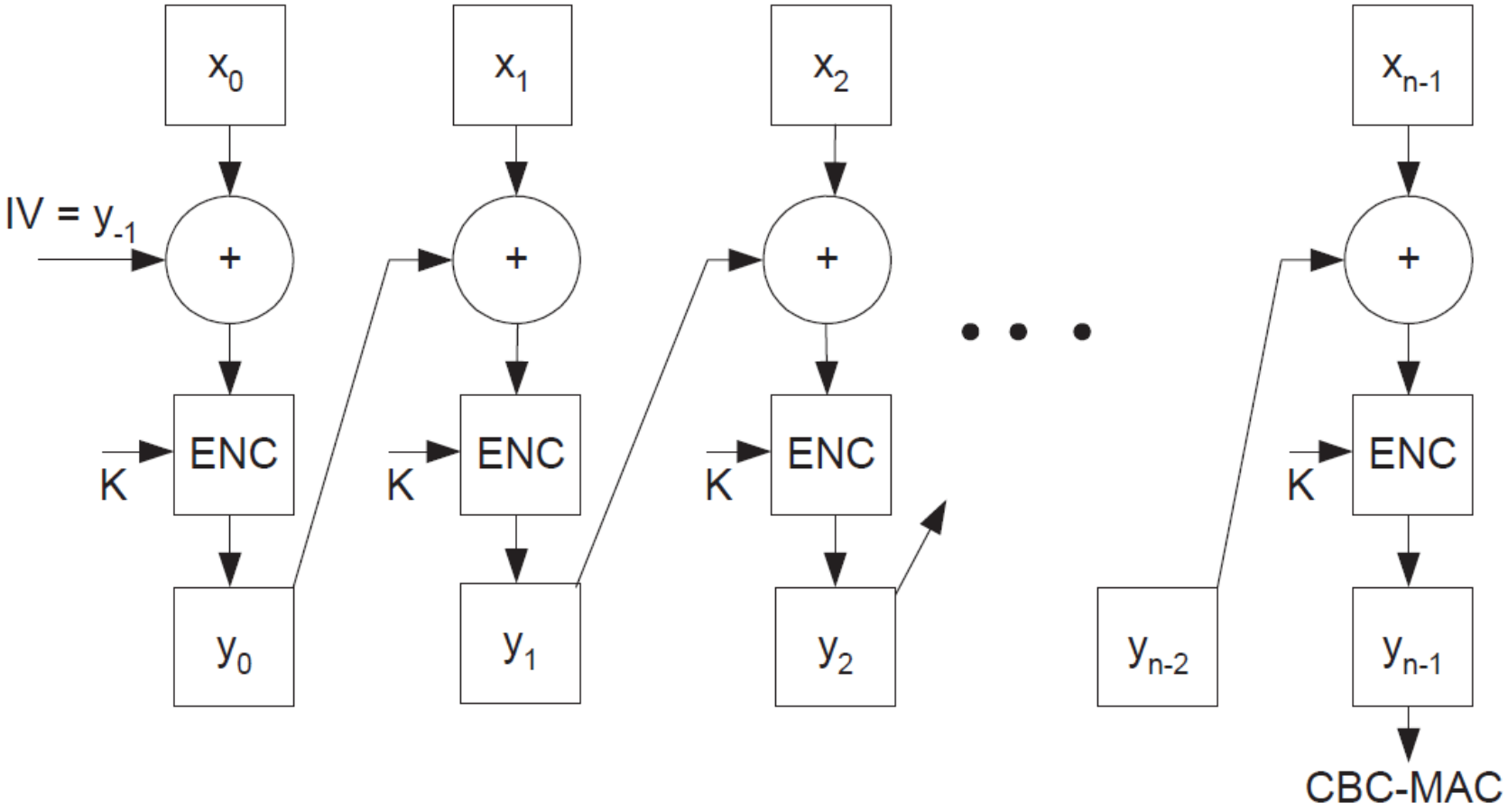
Properties of MAC

Two properties a MAC should have

- Key non-recovery: it is hard to compute the secret key from observed (message, MAC value) pairs.
- Computation resistance: even if many (message, MAC value) pairs are observed, it is hard to compute an as yet unobserved (message, MAC value) pair that verifies correctly.

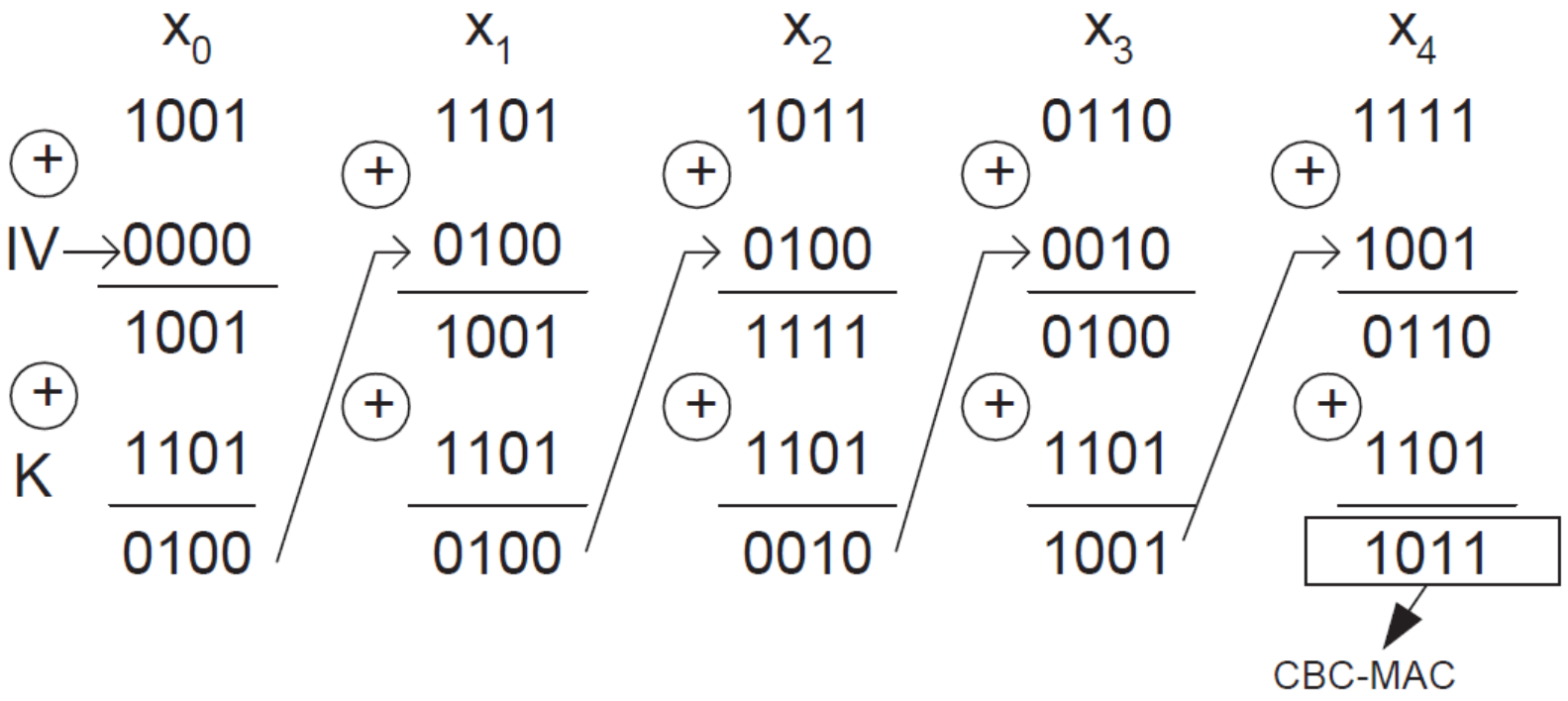


CBC-MAC



Example

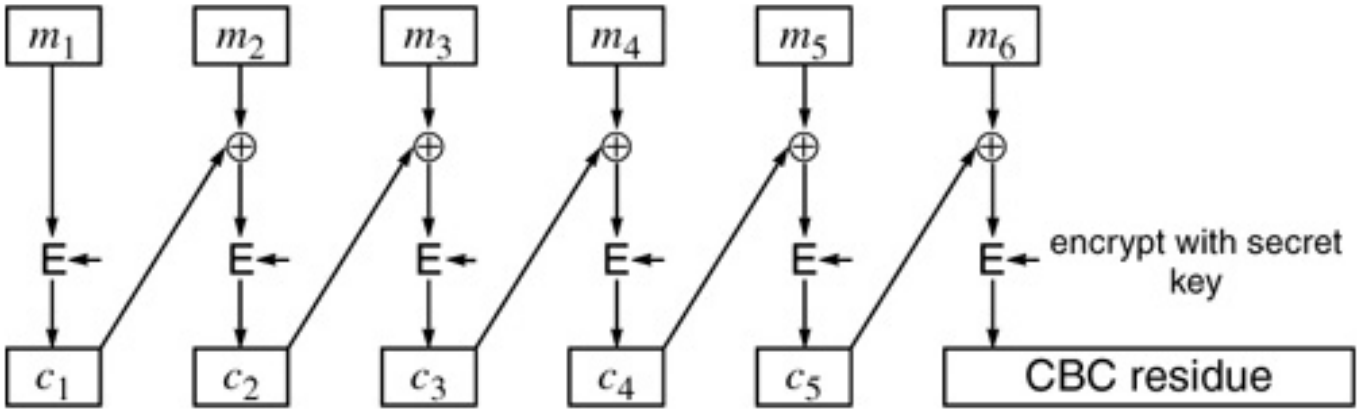
- How does Bob know the message length?
- Is this a good CBC-MAC?



Alice sends to Bob: 1001110110110110111**1011**

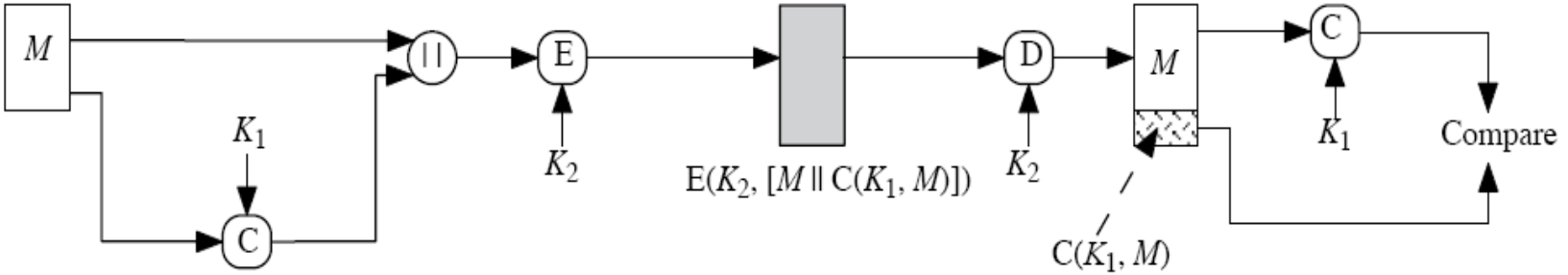
MACs based on Block Ciphers

- Protect against undetected modifications
- Plaintext + CBC residue (when message not secret)

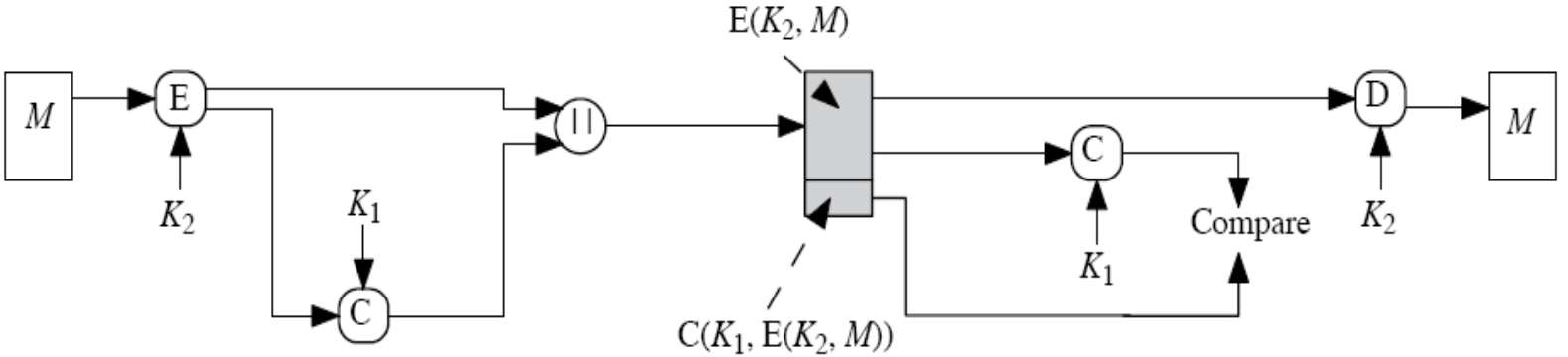


Authenticated Encryption

(a) Hash then Encrypt (not very secure)



(b) Message authentication and confidentiality; authentication tied to plaintext



(c) Message authentication and confidentiality; authentication tied to ciphertext

(d) Authentication (MAC) + Encryption (separately)

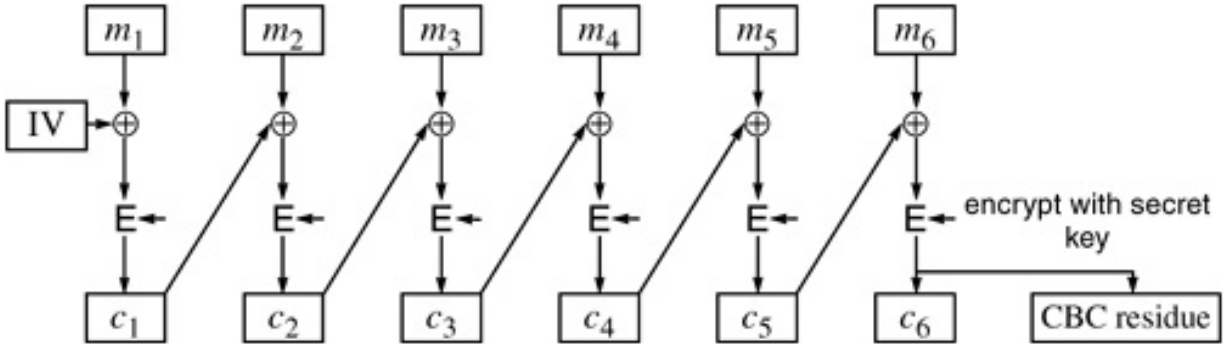
Authenticated Encryption based on Block Cipher Modes of Encryption

- Example:
  - Privacy: CBC encryption
  - Integrity: CBC residue

- Ciphertext + CBC residue ?
- Encrypt {plaintext + CBC residue} ?
- Encrypt {plaintext + CRC} ?

Ciphertext + CBC Residue

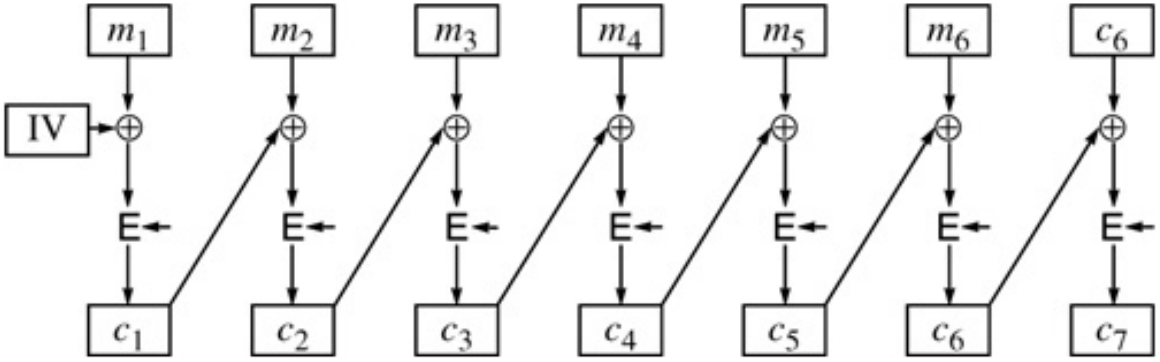
Figure 4-12. Cipher Block Chaining Encryption plus CBC Residue



- Problem?

Encrypt {plaintext + CBC residue}

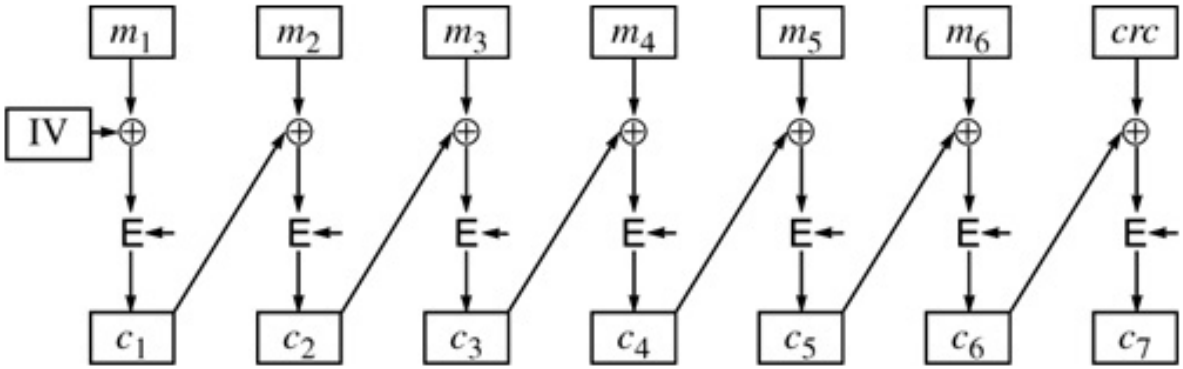
Figure 4-13. Cipher Block Chaining Encryption of Message with CBC Residue



- Problem?

Encrypt {plaintext + CRC}

Figure 4-14. Cipher Block Chaining Encryption of Message with CRC



- Longer CRC maybe Okay

Authenticated Encryption / Confidentiality and Integrity: The Do's

- Confidentiality: CBC encryption + Integrity: CBC residue, but with different keys
- CBC + weak cryptographic checksum
- CBC + cryptographic hash: keyed hash preferred
- CCM: Counter Mode + CMAC (A more secure version of CBC-MAC)
- ……