CS557: Cryptography

Message Authentication code (MAC)

S. Tripathy
IIT Patna

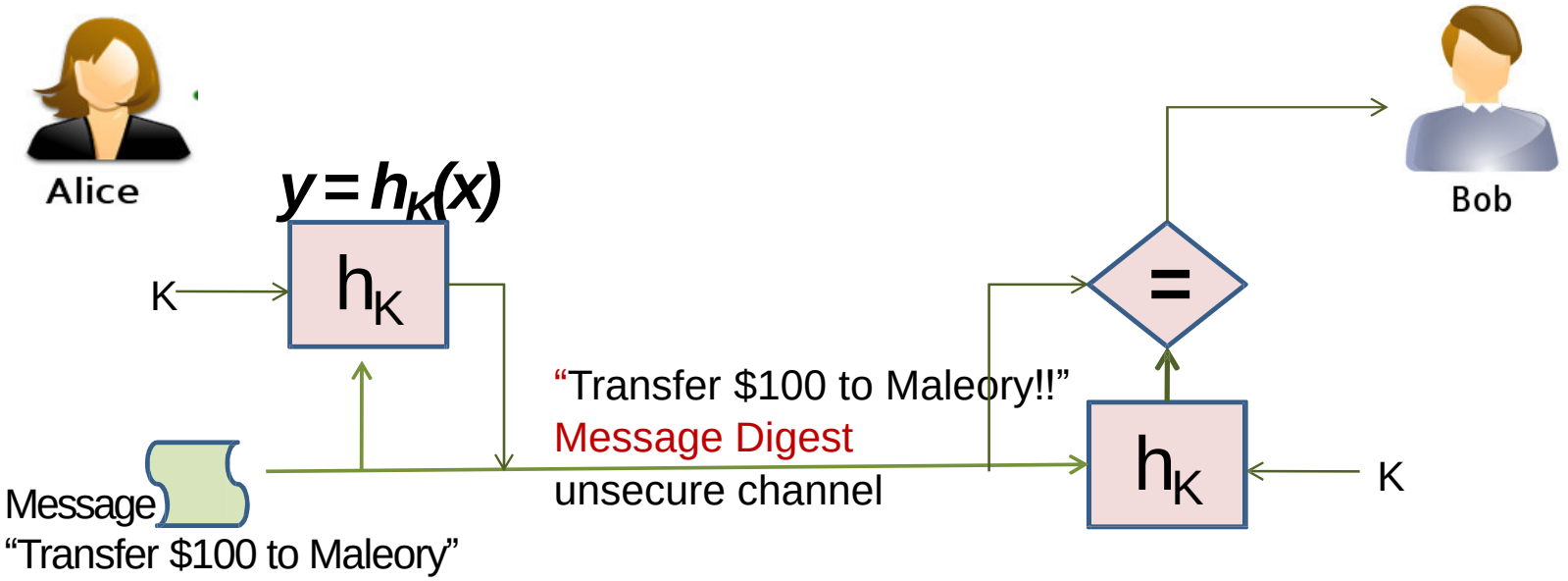
Previous Class

- Cryptography
  - Cryptographic Hash Function
    - One-way Hash function
    - Collision Resistant Hash Function
  - Cryptographic hash function
    - MD5, SHA1

Present Class

- Cryptography
  - Cryptographic (Keyed) Hash Function
    - MAC: Message Authentication code
      - CMAC, HMAC
  - Authenticated Encryption
    - CCM

Message Authentication Code (MAC)



MACs can allow the message and the digest to be sent over an insecure channel
However, it requires Alice and Bob to share a common key

- provides assurance that message is unaltered and comes from sender

Requirements for MACs

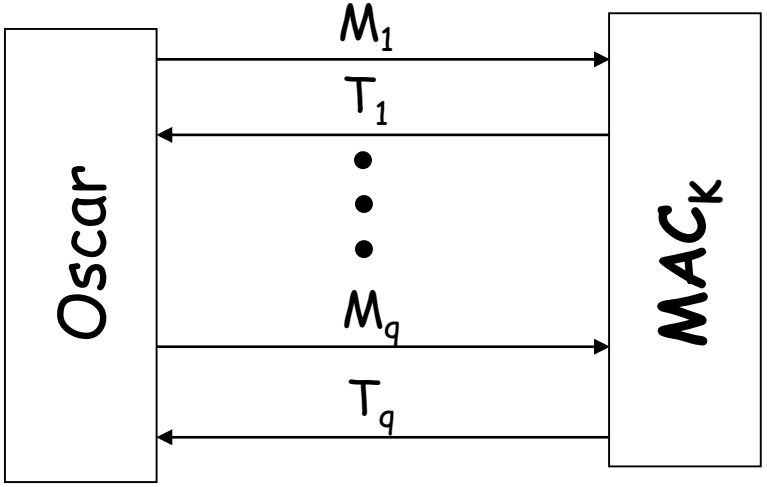
- taking into account the types of attacks MAC needs to satisfy the following:

1. knowing a message and MAC, it is infeasible to find another message with same MAC
2. MAC should depend equally on all bits of the message

3. MACs should be uniformly distributed

Distinguishing Attack

Stronger security notion than forging and Popular in the security analysis.



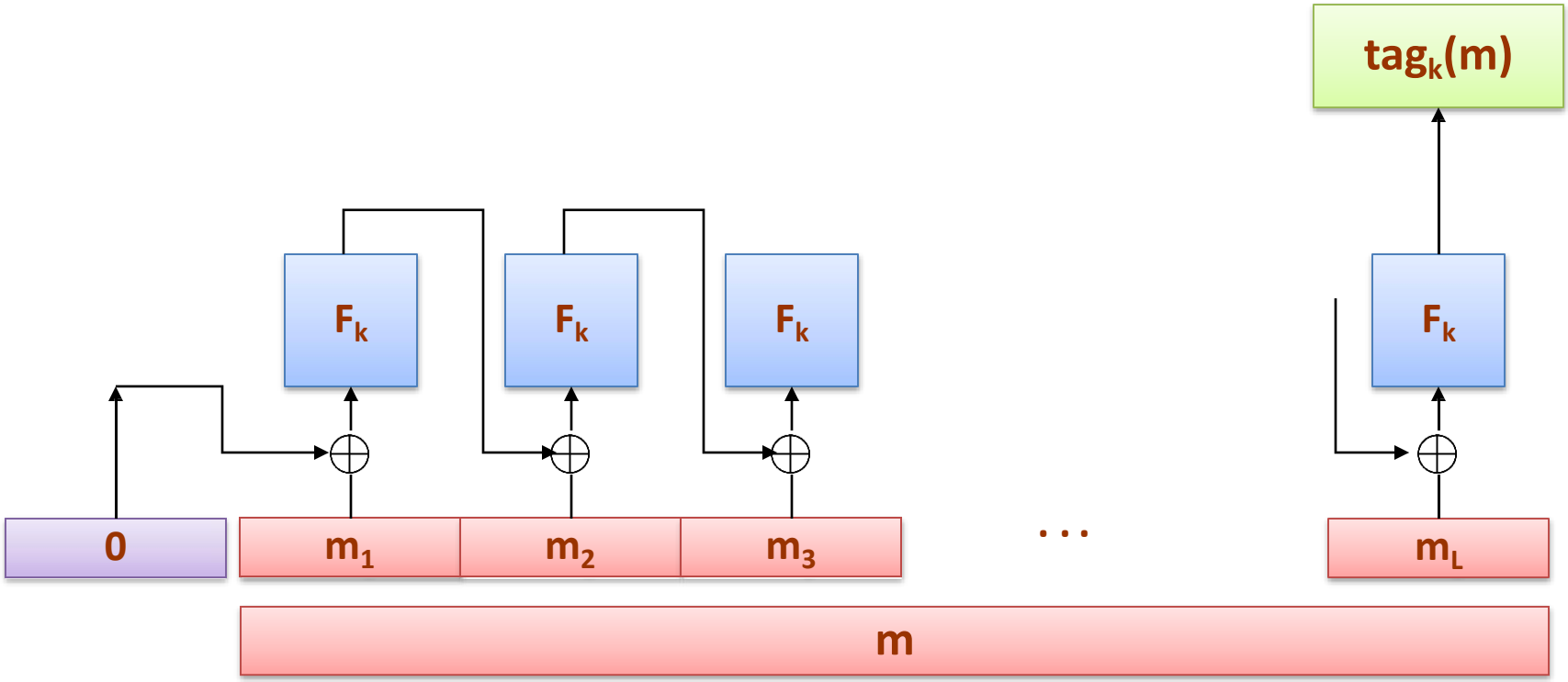
Finally, Oscar has to distinguish $\mathbf{T} = (T_1, \ldots, T_q)$ from a q-tuple of random strings.

Forgery in MAC

- Forgery: adversary creates a valid message and *MAC* pair that was not created by the legitimate signer.
- Existential forgery: The adversary creates a valid message and signature pair where the message can be anything, including gibberish.
- Selective Forgery: The adversary creates a valid message and signature pair where the message was chosen by the challenger before the attack.

CBC-MAC

$F : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ - a PRF



Theorem

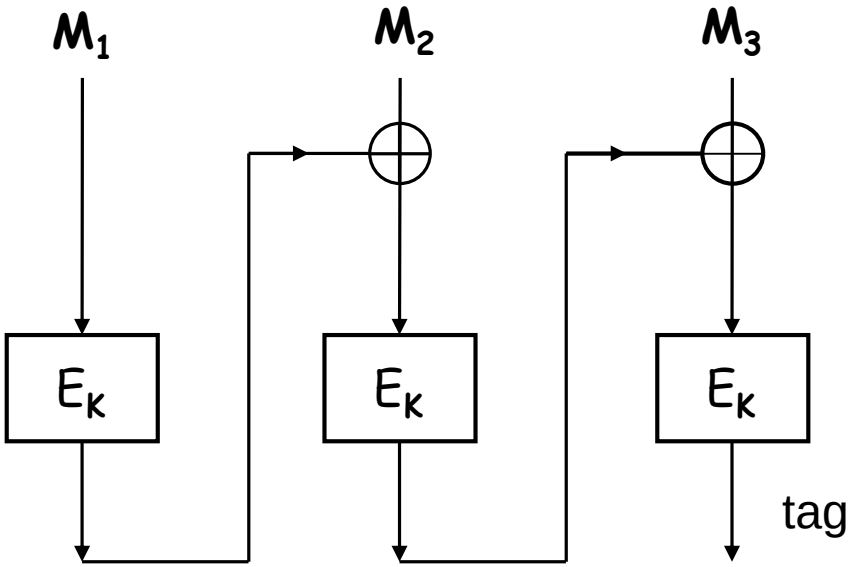
Assuming that $F : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$ is a PRF and messages of fixed length are tagged, then CBC-MAC construction is secure.

CBC-MAC vs CBC-Enc

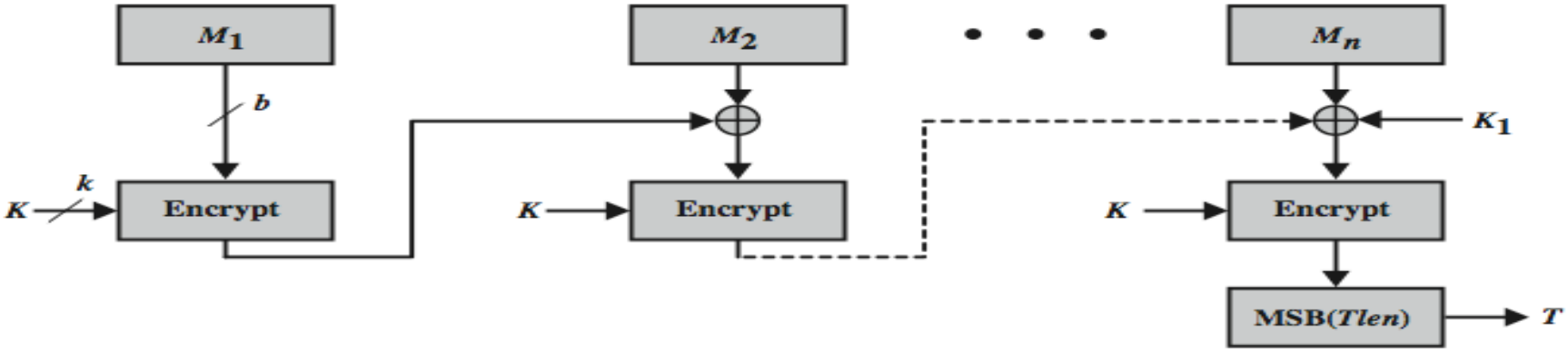
- Initialization
  - CBC-Enc uses random IV
  - CBC-MAC uses first block fixed at 0
  - CBC-MAC with random IV is insecure!
- Output
  - CBC-Enc outputs all intermediate blocks (to decrypt)
  - CBC-MAC outputs only last block
- Different security properties
  - CBC-Enc is CPA secure encryption
  - CBC-MAC is secure MAC

CBC-MAC: Block Cipher based MAC

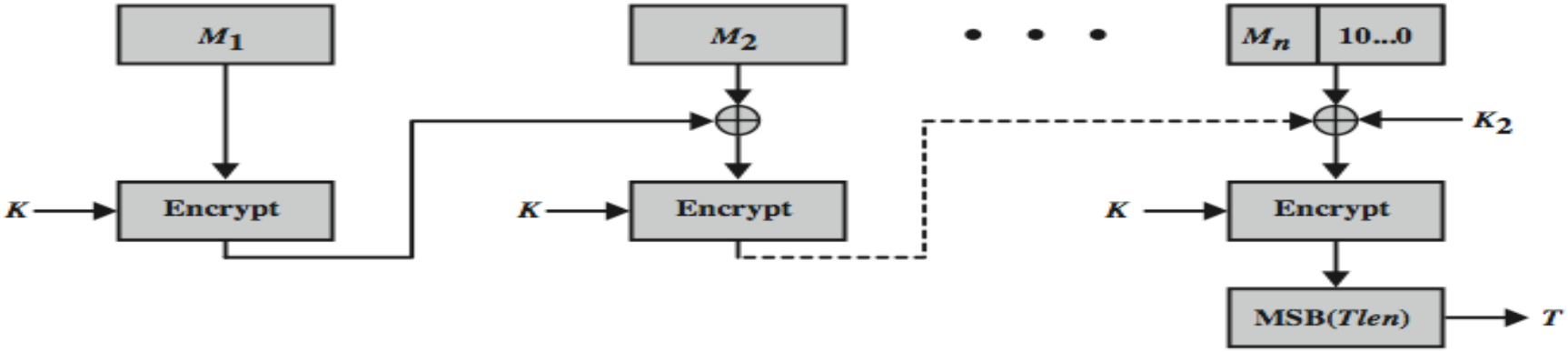
- CBC MAC secure for prefix-free message space only.
- Secure for fixed length
- Length extension attack is valid for arbitrary domain



MAC using Block cipher (CMAC: Cipher based message authentication code)



(a) Message length is integer multiple of block size



(b) Message length is not integer multiple of block size

- Thanks