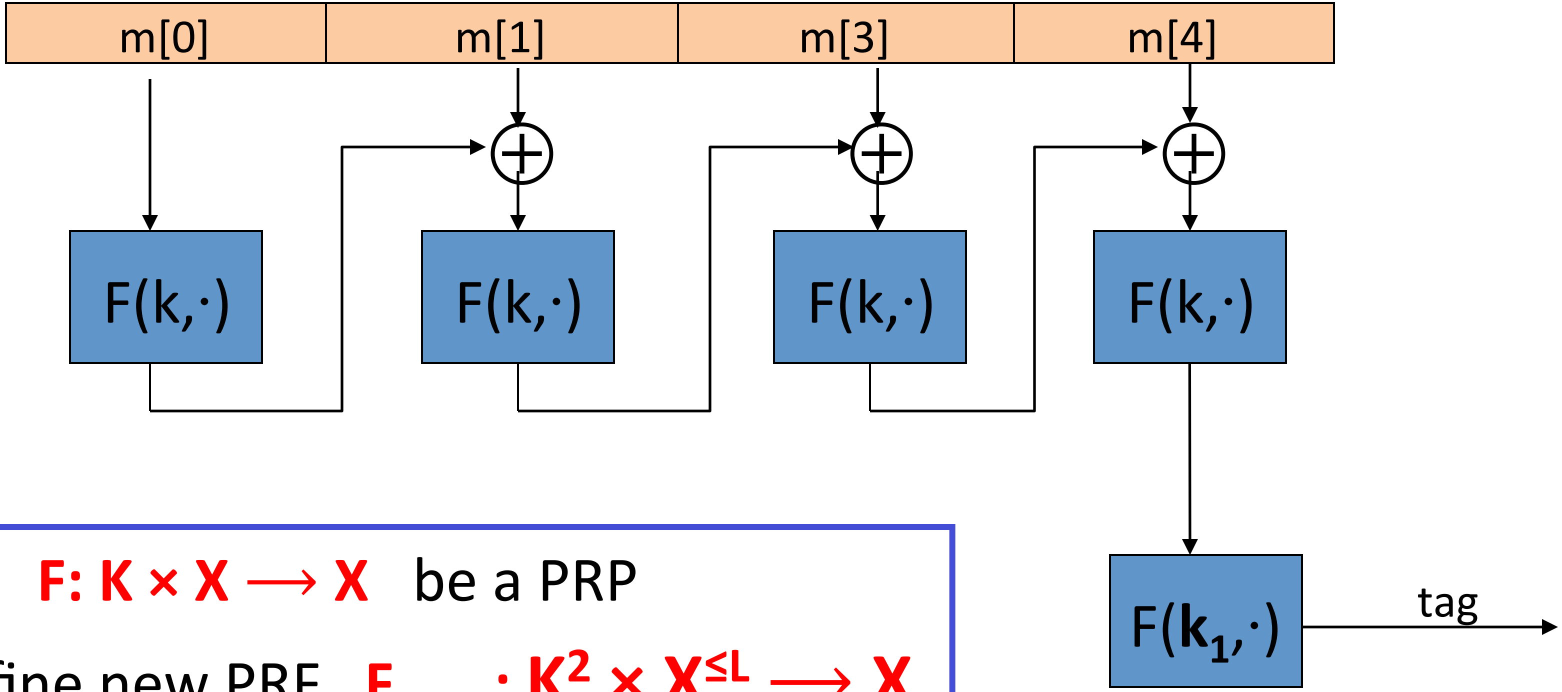
Message Integrity

MAC padding

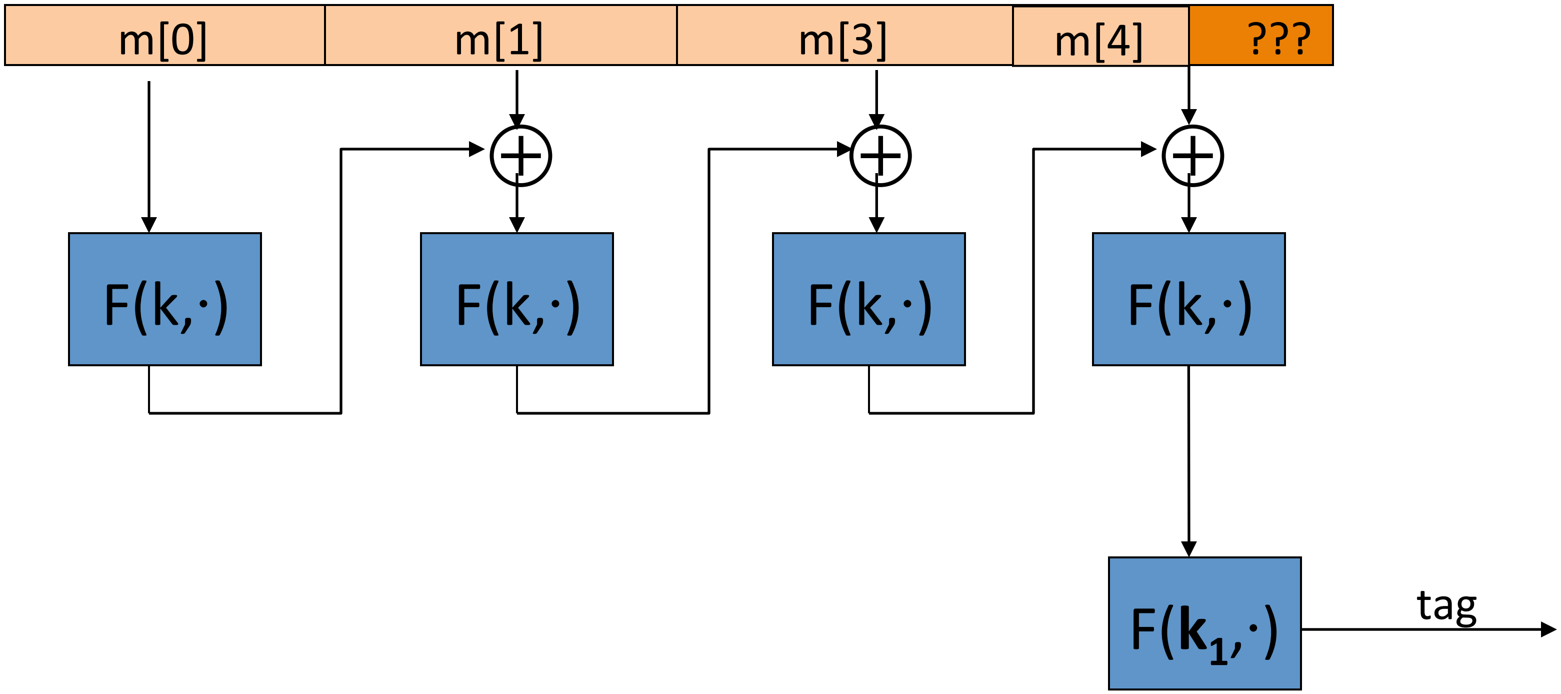
Recall: ECBC-MAC



Let $\mathbf{F: K \times X \longrightarrow X}$ be a PRP

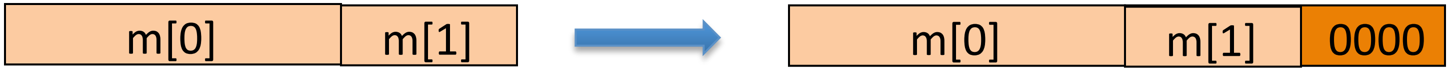
Define new PRF $\mathbf{F_{ECBC} : K^2 \times X^{\leq L} \longrightarrow X}$

What if msg. len. is not multiple of block-size?



CBC MAC padding

Bad idea: pad m with 0's



Is the resulting MAC secure?

- ○ Yes, the MAC is secure
- ○ It depends on the underlying MAC
- ○ [✓ No, given tag on msg **m** attacker obtains tag on **m||0**]
- ○

Problem: pad(m) = pad(m||0)

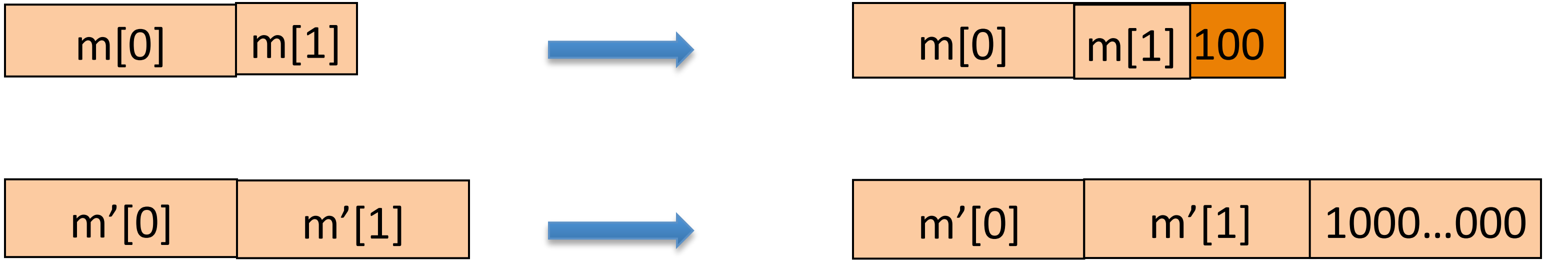
CBC MAC padding

For security, padding must be invertible !

$$m_0 \neq m_1 \quad \Rightarrow \quad \text{pad}(m_0) \neq \text{pad}(m_1)$$

ISO: pad with "1000…00". Add new dummy block if needed.

- The "1" indicates beginning of pad.

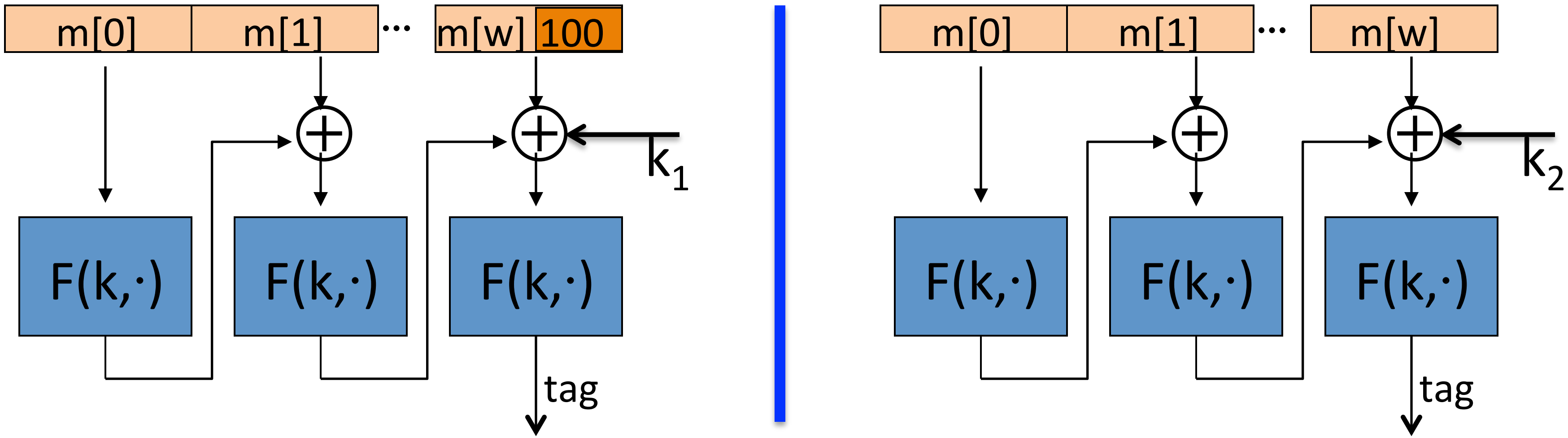


CMAC (NIST standard)

(k_1, k_2) derived from k

Variant of CBC-MAC where key = (k, k_1, k_2)

- No final encryption step (extension attack thwarted by last keyed xor)
- No dummy block (ambiguity resolved by use of k_1 or k_2)



End of Segment