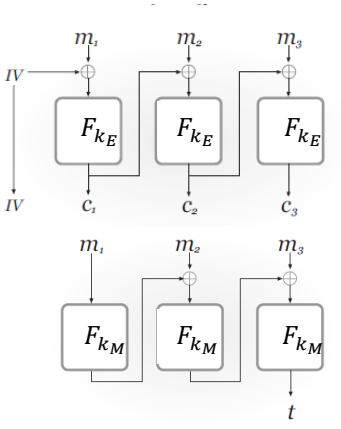
Class Exercise—Authenticated Encryption
ENEE 457/CMSC 498E
11/01/17

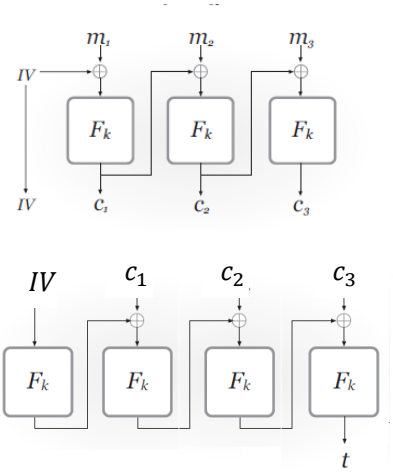
Consider the following approaches for combining CBC-ENC with CBC-MAC. For each one, explain why the approach is insecure. I.e. each approach will either compromise message privacy or message authentication/integrity. In both cases, assume that we are trying to construct a fixed-length authenticated encryption scheme were it is known that all messages will consist of exactly three blocks.

1. Run CBC-ENC and CBC-MAC in parallel on the message m:



Output: (IV, c_1, c_2, c_3, t)

2. First run CBC-ENC, then run CBC-MAC on the ciphertext, but use the *same* key for both.



Output: (IV, c_1, c_2, c_3, t)