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:

   To break CPA security query m₀, get back (c₀, t₀).
   Now submit (m₀, m₁) to the challenge.
   Get back (c*₀, t*₀).
   If t₀ = t₀, output b' = 0
   o/w output b' = 1
   The attacker always guesses correctly.

   **CBC-Enc**
   \[
   \begin{array}{c}
   \text{iv} \\
   \downarrow \\
   m₀ \\
   \downarrow \\
   c₀ \\
   \downarrow \\
   c₁ \\
   \downarrow \\
   c₂ \\
   \downarrow \\
   c₃ \\
   \downarrow \\
   t₀ \\
   \end{array}
   \]
   \[
   \begin{array}{c}
   \text{iv} \\
   \downarrow \\
   m₁ \\
   \downarrow \\
   c₁ \\
   \downarrow \\
   c₂ \\
   \downarrow \\
   c₃ \\
   \downarrow \\
   t₁ \\
   \end{array}
   \]
   \[
   \begin{array}{c}
   \text{iv} \\
   \downarrow \\
   m₂ \\
   \downarrow \\
   c₂ \\
   \downarrow \\
   c₃ \\
   \downarrow \\
   t₂ \\
   \end{array}
   \]
   \[
   \begin{array}{c}
   \text{iv} \\
   \downarrow \\
   m₃ \\
   \downarrow \\
   c₃ \\
   \downarrow \\
   t₃ \\
   \end{array}
   \]

   **CBC-Mac**
   \[
   \begin{array}{c}
   \downarrow \\
   \text{iv} \\
   \downarrow \\
   m₀ \\
   \downarrow \\
   c₀ \\
   \downarrow \\
   c₁ \\
   \downarrow \\
   c₂ \\
   \downarrow \\
   c₃ \\
   \downarrow \\
   t₀ \\
   \end{array}
   \]
   \[
   \begin{array}{c}
   \downarrow \\
   \text{iv} \\
   \downarrow \\
   m₁ \\
   \downarrow \\
   c₁ \\
   \downarrow \\
   c₂ \\
   \downarrow \\
   c₃ \\
   \downarrow \\
   t₁ \\
   \end{array}
   \]
   \[
   \begin{array}{c}
   \downarrow \\
   \text{iv} \\
   \downarrow \\
   m₂ \\
   \downarrow \\
   c₂ \\
   \downarrow \\
   c₃ \\
   \downarrow \\
   t₂ \\
   \end{array}
   \]
   \[
   \begin{array}{c}
   \downarrow \\
   \text{iv} \\
   \downarrow \\
   m₃ \\
   \downarrow \\
   c₃ \\
   \downarrow \\
   t₃ \\
   \end{array}
   \]

   note: CBC-Mac is deterministic

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

   To break Unforgeability query (m₁, m₂, m₃).
   Get back (IV, c₁, c₂, c₃).
   Now we know the following about Fₖ:
   1. Fₖ(IV ⊕ m₁) = c₁
   2. Fₖ(c₁ ⊕ m₂) = c₂
   3. Fₖ(c₂ ⊕ m₃) = c₃

   We will choose (IV', c₁', c₂', c₃') such that all values of A, B, C, t' are known.
   Output: (IV, c₁, c₂, c₃, t)

   This means that (IV', c₁', c₂', c₃', t') breaks unforgeability.

   1. Set IV' = IV ⊕ m₁ then A = c₁
   2. Set c₁' = c₁ ⊕ c₂ ⊕ m₃ then B = c₃
   3. Set c₂' = c₁ ⊕ m₂ ⊕ c₃ then C = c₂
   4. Set c₃' = IV ⊕ m₁ ⊕ c₂; t' = c₁