COSC 530: Homework 3

Problem 1. (30 points.)

(Part A - 20 points.) Many of the encryption and message authentication schemes we have seen use a key consisting of two keys for the underlying blockcipher (e.g., ECBC-MAC, and all of the generic composition methods for AE). Give a generic transformation that when applied to such a scheme gives a new scheme that remains secure but uses a key consisting of only one key for the underlying blockcipher.

(Part B - 10 points.) Why are tailored one-key schemes more desirable than one-key schemes obtained from your generic transformation — e.g., why is CMAC more desirable than the scheme obtained by applying your generic transformation to ECBC-MAC?

Problem 2. (70 points.) Define SE = (K, E, D) where K returns a random 128-bit key K and

**Algorithm EK(M):**
- If |M| ≠ 512 then return ⊥
- Ce[0] ← {0, 1}128; Cm[0] ← 0128
- For i = 1, 2, 3, 4 do:
  - Ce[i] ← AESK(Ce[i - 1] ⊕ M[i])
  - Cm[i] ← AESK(Cm[i - 1] ⊕ M[i])
- T ← Cm[4]; Return (Ce, T)

**Algorithm DK((Ce, T)):**
- If |Ce| ≠ 640 then return ⊥
- Cm[0] ← {0, 1}128
- For i = 1, 2, 3, 4 do:
  - M[i] ← AESK−1(Ce[i]) ⊕ Ce[i - 1]
  - Cm[i] ← AESK(Cm[i - 1] ⊕ M[i])
- Else return ⊥

(Part A - 30 points.) Is SE IND-CPA secure?

(Part B - 30 points.) Is SE INT-CTXT secure?

(Part C - 10 points.) Is SE obtained via the Encrypt-and-MAC generic composition method on some underlying symmetric-key encryption scheme and message authentication code?

For Parts A and B above, if your answer is “yes” then you should give some convincing intuition (a proof is best, but not necessary for full credit). You can make the usual assumptions about the security of AES. If your answer is “no” then you should give an explicit attack.