Problem 1.  (30 points.) Recall that generic composition methods for building an authenticated encryption scheme from a symmetric-key encryption scheme and PRF yield an authenticated encryption scheme whose key consists of two keys, one for the symmetric-key encryption scheme and one for the PRF. Sketch a transformation that when applied to such an authenticated encryption scheme gives a new scheme that remains secure but instead uses a key consisting of only one key for an underlying blockcipher, e.g., AES. I am looking for a clear description of how to generate the two keys used by the authenticated encryption scheme from one key for the underlying blockcipher. You do not need to justify your answer.

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

$$\text{Algorithm } \mathcal{E}_K(M):$$

If $|M| \neq 512$ then return $\bot$


$C_e[0] \leftarrow \{0, 1\}^{128}; C_m[0] \leftarrow 0^{128}$

For $i = 1, 2, 3, 4$ do:

$C_e[i] \leftarrow \text{AES}_K(C_e[i-1] \oplus M[i])$

$C_m[i] \leftarrow \text{AES}_K(C_m[i-1] \oplus M[i])$


$T \leftarrow C_m[4]; \text{ Return } (C_e, T)$

$$\text{Algorithm } \mathcal{D}_K((C_e, T)):$$

If $|C_e| \neq 640$ then return $\bot$

$C_m[0] \leftarrow \{0, 1\}^{128}$

For $i = 1, 2, 3, 4$ do:

$M[i] \leftarrow \text{AES}^{-1}_K(C_e[i]) \oplus C_e[i-1]$

$C_m[i] \leftarrow \text{AES}_K(C_m[i-1] \oplus M[i])$


Else return $\bot$

(Part A - 30 points.) Is $\mathcal{SE}$ IND-CPA secure?

(Part B - 30 points.) Is $\mathcal{SE}$ INT-CTXT secure?

(Part C - 10 points.) Can one view $\mathcal{SE}$ as obtained by applying the Encrypt-and-MAC generic composition method on some underlying symmetric-key encryption scheme and PRF?

For Parts A and B above, if your answer is “yes” then you should give some convincing intuition. You can make the usual assumptions about the security of AES. If your answer is “no” then you should give an explicit attack.