# COMPSCI-466: Homework 6

**Problem 1.** (100 points.) Define $\mathsf{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ where $\mathcal{K}$ returns a random 128-bit key $K$ and

**Algorithm** $\mathcal{E}_K(M)$:
If $|M| \neq 512$ then return $\perp$
$M[1]\|M[2]\|M[3]\|M[4] \leftarrow M$
$C_e[0] \leftarrow\!\!\$\ \{0,1\}^{128}$ ; $C_m[0] \leftarrow 0^{128}$
For $i = 1, 2, 3, 4$ do:
$C_e[i] \leftarrow \mathsf{AES}_K(C_e[i-1] \oplus M[i])$
$C_m[i] \leftarrow \mathsf{AES}_K(C_m[i-1] \oplus M[i])$
$C_e \leftarrow C_e[0]\|C_e[1]\|C_e[2]\|C_e[3]\|C_e[4]$
$T \leftarrow C_m[4]$ ; Return $(C_e, T)$

**Algorithm** $\mathcal{D}_K((C_e, T))$:
If $|C_e| \neq 640$ then return $\perp$
$C_m[0] \leftarrow 0^{128}$
For $i = 1, 2, 3, 4$ do:
$M[i] \leftarrow \mathsf{AES}_K^{-1}(C_e[i]) \oplus C_e[i-1]$
$C_m[i] \leftarrow \mathsf{AES}_K(C_m[i-1] \oplus M[i])$
If $C_m[4] = T$ then return $M[1]\|M[2]\|M[3]\|M[4]$
Else return $\perp$

(Part A - 40 points.) Is $\mathsf{SE}$ IND-CPA secure?

(Part B - 40 points.) Is $\mathsf{SE}$ INT-CTXT secure?

(Part C - 20 points.) Is $\mathsf{SE}$ obtained via the Encrypt-and-MAC generic composition method on some underlying symmetric-key encryption scheme and PRF? Justify your answer.

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, meaning pseudocode for an adversary and analysis of its advantage and run-time.