Problem Set 4

For this problem set, assume the following building blocks. Let n be a positive integer, and let $E : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher secure under the PRF security notion. Recall the counter mode encryption CTRC scheme $(\mathsf{KG}, \mathsf{CTRC\text{-}Enc}, \mathsf{CTRC\text{-}Dec})$ studied in class. The pseudocode for the encryption algorithm $\mathsf{CTRC\text{-}Enc}$ is included here for your convenience. We will use the version where the very first block cipher application is performed on 0. (See the body of the for loop.) As usual, in the pseudocode we assume automatic type conversion between integers and their binary representation as bitstrings to avoid cluttering up our pseudocode. (For example, $C[0]$ is a bitstring even though its value comes from ctr, which is an integer. The automatic type conversion is assumed here.)

Algorithm $\mathsf{CTRC\text{-}Enc}(K, M)$
  If $(|M| = 0)$ or $(|M| \bmod n \neq 0)$ then return $\perp$
  Parse M as n-bit blocks $M[1] \ldots M[m]$
  $\mathsf{static}\ ctr \leftarrow 0$
  $C[0] \leftarrow ctr$; $ctr \leftarrow ctr + m$
  If $ctr - 1 > 2^n - 1$ then return $\perp$
  For $i = 1$ to m do $C[i] \leftarrow E_K(C[0] + i - 1) \oplus M[i]$
  Return $C[0] \ldots C[m]$

You may use without proof the fact that PRFs make good MACs. That is, you may assume that, if E is a block cipher as defined above and if KG is the usual key generation algorithm (namely, an algorithm that simply returns a uniform randomly chosen bitstring of length n), the following construction yields a MAC scheme $\mathsf{MA} = (\mathsf{KG}, \mathsf{PRF\text{-}Tag})$ secure under the SUF-CMA security notion.

Algorithm $\mathsf{PRF\text{-}Tag}(K, M)$
  If $(|M| = 0)$ or $(|M| \neq n)$ then return $\perp$
  Return $E_K(M)$

Note that since this tagging algorithm is deterministic and stateless, we do not need to specify the verification algorithm. (It simply recomputes the tag and compares the result with the tag that it has received.)

1. Consider an authenticated encryption scheme $\mathsf{AE1} = (\mathsf{KG}', \mathcal{E}', \mathcal{D}')$ defined as follows.

Algorithm KG'	Algorithm $\mathcal{E}'(K_1K_2, M)$	Algorithm $\mathcal{D}'(K_1K_2, C)$
$K_1 \xleftarrow{\$} \{0,1\}^n$	Parse M into n-bit blocks $M[1]\ldots M[m]$	Parse C into n-bit blocks $C[0]\ldots C[m]T$
$K_2 \xleftarrow{\$} \{0,1\}^n$	$s \leftarrow M[1] \oplus \ldots \oplus M[m]$	$M \leftarrow \mathsf{CTRC\text{-}Dec}(K_1, C[0]\ldots C[m])$
Return $K_1 \Vert K_2$	Return $\mathsf{CTRC\text{-}Enc}(K_1, M) \Vert \mathsf{PRF\text{-}Tag}(K_2, s)$	If $M = \perp$ return $\perp$
		Parse M into n-bit blocks $M[1]\ldots M[m]$
		$s \leftarrow M[1] \oplus \ldots \oplus M[m]$
		If $T = \mathsf{PRF\text{-}Tag}(K_2, s)$ return M
		Return $\perp$

(a) Is $\mathsf{AE1}$ secure under the IND-CPA security notion?

(b) Prove your answer to the previous question. Be sure to provide a complete proof. Specifically, if you answer yes, specify a reduction along with an analysis relating the advantages of relevant adversaries and their resource usage. If you answer no, specify a counterexample, an attack, and an analysis of the adversary's advantage and resource usage. As always, an adversary requiring a minimal amount of resources while achieving a high advantage value is better.

(c) Is $\mathsf{AE1}$ secure under the INT-CTXT security notion?

(d) Prove your answer to the previous question. Be sure to provide a complete proof. Specifically, if you answer yes, specify a reduction along with an analysis relating the advantages of relevant adversaries and their resource usage. If you answer no, specify a counterexample, an attack, and an analysis of the adversary's advantage and resource usage. As always, an adversary requiring a minimal amount of resources while achieving a high advantage value is better.

2. Define an encryption scheme $\mathsf{SE} = (\mathsf{KG}, \mathcal{E}, \mathcal{D})$ as follows.

Algorithm KG	Algorithm $\mathcal{E}(K, M)$	Algorithm $\mathcal{D}(K, C)$
$K \xleftarrow{\$} \{0,1\}^n$	Return $0 \Vert \mathsf{CTRC\text{-}Enc}(K, M)$	Parse C as $b \Vert C'$ where b is a bit
Return K		Parse C' into n-bit blocks $C[0]\ldots C[m]$
		$M \leftarrow \mathsf{CTRC\text{-}Dec}(K, C[0]\ldots C[m])$
		Return M

Let $\mathsf{MA} = (\mathsf{KG}, \mathsf{Tag}, \mathsf{Vf})$ be an SUF-CMA secure MAC scheme, and let each tag produced by Tag be of length t. Define an authenticated encryption scheme $\mathsf{AE2} = (\mathsf{KG}', \mathcal{E}', \mathcal{D}')$ as follows.

Algorithm KG'	Algorithm $\mathcal{E}'(K_1K_2, M)$	Algorithm $\mathcal{D}'(K_1K_2, C)$
$K_1 \xleftarrow{\$} \{0,1\}^n$	Return $\mathcal{E}(K_1, M \Vert \mathsf{Tag}(K_2, M))$	$M' \leftarrow \mathcal{D}(K_1, C)$
$K_2 \xleftarrow{\$} \{0,1\}^n$		If $M' = \perp$ return $\perp$
Return $K_1 \Vert K_2$		Parse M' into $M \Vert T$ where $\lvert T \rvert = t$
		Return $\mathsf{Vf}(K_2, M, T)$

(a) Is $\mathsf{AE2}$ secure under the INT-CTXT security notion?

(b) Prove your answer to the previous question. Be sure to provide a complete proof. Specifically, if you answer yes, specify a reduction along with an analysis relating the advantages of relevant adversaries and their resource usage. If you answer no, specify a counterexample, an attack, and an analysis of the adversary's advantage and resource usage. As always, an adversary requiring a minimal amount of resources while achieving a high advantage value is better.

3. Let $\mathsf{MA} = (\mathsf{KG}, \mathsf{Tag}, \mathsf{Vf})$ be an SUF-CMA secure MAC scheme, and let each tag produced by Tag be of length t. Define an authenticated encryption scheme $\mathsf{AE3} = (\mathsf{KG}', \mathcal{E}', \mathcal{D}')$ as follows.

Algorithm KG'	Algorithm $\mathcal{E}'(K_1K_2, M)$	Algorithm $\mathcal{D}'(K_1K_2, C')$
$K_1 \xleftarrow{\$} \{0,1\}^n$	$C' \xleftarrow{\$} \mathsf{CTRC\text{-}Enc}(K_1, M)$	Parse C' as $\mathsf{IV}\\|C\\|T$
$K_2 \xleftarrow{\$} \{0,1\}^n$	Parse C' as IV and C where $\|\mathsf{IV}\| = n$	where $\|\mathsf{IV}\| = n$ and $\|T\| = t$
Return $K_1\\|K_2$	$T \xleftarrow{\$} \mathsf{Tag}(K_2, C)$	If $\mathsf{Vf}(K_2, C, T) \neq 1$ return $\perp$
	Return $\mathsf{IV}\\|C\\|T$	$M \leftarrow \mathsf{CTRC\text{-}Dec}(K_1, \mathsf{IV}\\|C)$
		Return M

(a) Is $\mathsf{AE3}$ secure under the INT-CTXT security notion?

(b) Prove your answer to the previous question. Be sure to provide a complete proof. Specifically, if you answer yes, specify a reduction along with an analysis relating the advantages of relevant adversaries and their resource usage. If you answer no, specify a counterexample, an attack, and an analysis of the adversary's advantage and resource usage. As always, an adversary requiring a minimal amount of resources while achieving a high advantage value is better.