COSC531: Homework 3

Three problems, 120 points total.

Let $\text{MsgSp}$ be a message space and $p: \text{MsgSp} \times \text{MsgSp} \rightarrow \{0, 1\}$ be a binary predicate on $\text{MsgSp}$. Define a $p$-revealing encoding scheme to be a tuple $(\text{KeyGen}, \text{Encode}, \text{Eval})$ where $\text{KeyGen}$ is a randomized key-generation algorithm that outputs a key $K$, $\text{Encode}$ is a randomized encoding algorithm that on inputs a key $K$ and message $m$ outputs an encoding $e$, and $\text{Eval}$ is a deterministic evaluation algorithm that on inputs an encoding $e_1$ and another encoding $e_2$ outputs a bit $b$. For correct evaluation we require that for all $K$ output by $\text{KeyGen}$ and all messages $m_1, m_2 \in \text{MsgSp}$

$$\Pr \left[ \text{Eval}(\text{Encode}(K, m_1), \text{Encode}(K, m_2)) \text{ outputs } p(m_1, m_2) \right] = 1.$$  

Define a $p$-revealing encryption scheme to be like a $p$-revealing encoding scheme except encodings are decryptable. That is, define a $p$-revealing encryption scheme to be a tuple $(\text{KeyGen}, \text{Enc}, \text{Dec}, \text{Eval})$ where $(\text{KeyGen}, \text{Enc}, \text{Eval})$ is a (correct) $p$-revealing encoding scheme (except we call an encoding a ciphertext and denote it by $c$) and $(\text{KeyGen}, \text{Enc}, \text{Dec})$ is a (correct) symmetric-key encryption scheme (where correctness refers to correct decryption).

**Problem 1.** (15 points.) Let $\Pi = (\text{KeyGen}, \text{Encode}, \text{Eval})$ be a $p$-revealing encoding scheme (for $\text{MsgSp}$ and $p$ as above). We define an indistinguishability-style security definition like those usually given in class, to capture the intuition that the scheme should leak only $p$. To an adversary $A$ we associate the experiment

$\text{Experiment } \text{Exp}_\Pi^{\text{ind}}(A)$:

\[
K \leftarrow \mathcal{K} \\
\hat{b}' \leftarrow A^{\text{Enc}(K, (\mathcal{CR}(\cdot, b)))} \\
\text{If } b = \hat{b}' \text{ then return } 1 \\
\text{Else return } 0
\]

We then associate to $A$ its IND-advantage against $\Pi$, defined as

$$\text{Adv}_{\Pi}^{\text{ind}}(A) := 2 \cdot \Pr \left[ \text{Exp}_{\Pi}^{\text{ind}}(A) \text{ outputs } 1 \right] - 1.$$  

We say that $A$ is $p$-legitimate if in any run of $\text{Exp}_{\Pi}^{\text{ind}}(A)$ its oracle queries $(m^1_0, m^1_1), \ldots, (m^q_0, m^q_1)$ satisfy

$$\ldots$$

We then say that $\Pi$ is IND-$p$CPA secure if for any “efficient” $p$-legitimate adversary its advantage $\text{Adv}_{\Pi}^{\text{ind}}(A)$ against $\Pi$ is “small.”

Fill in the “…” condition above to give the right definition of $p$-legitimate here.
Problem 2. (70 points.) Let \( \Pi = (\text{KeyGen, Enc, Dec, Eval}) \) be a \( p \)-revealing encryption scheme. We say that \( \Pi \) is IND-\( p \)CPA secure if the encoding scheme \( (\text{KeyGen, Enc, Eval}) \) is IND-\( p \)CPA secure.

Construct an IND-\( p \)CPA secure \( p \)-revealing encryption scheme \( \Pi = (\text{KeyGen, Enc, Dec, Eval}) \) from any IND-\( p \)CPA secure \( p \)-revealing encoding scheme \( \Pi = (\text{KeyGen, Encode, Eval}) \). That is, your solution should consist of the pseudocode for the algorithms of \( \Pi \). In addition to \( \Pi \), you can use any standard cryptographic primitives defined in class in your construction, as long as you use the correct syntax for them.

You do not have to prove security of your construction. However, doing so (i.e., giving a reduction from IND-\( p \)CPA security of \( \Pi \) to IND-\( p \)CPA security of \( \Pi \) and the appropriate security notions of whatever other primitives you use) is worth 50 extra credit points.

Problem 3. (35 points.) Define an order-revealing encryption scheme to be a \( p \)-revealing encryption scheme in which \( \text{MsgSp} = \{1, \ldots, M\} \) for some \( M \in \mathbb{N} \) and \( p(m_1, m_2) = 1 \) iff \( m_1 \leq m_2 \). Note that for such schemes, IND-\( p \)CPA security coincides with the notion of IND-OCPA security defined in class. In class, we showed that an order-preserving encryption scheme cannot be IND-OCPA security unless its ciphertexts are \( \Omega(M) \)-bits long. (Thus if \( M = 2^k \), a ciphertext is roughly \( 2^k \)-bits long.) Does the same argument apply to order-revealing encryption? Give precise reasoning why or why not. (If the argument fails, pinpoint exactly why.)