Problem Set 2

1. Let $E : \{0,1\}^2 \times \{0,1\}^3 \to \{0,1\}^3$ be the following block cipher.

$$\begin{array}{llll} E_{00} & = (100, 110, 010, 000, 101, 111, 011, 001) & E_{01} & = (001, 010, 000, 111, 110, 011, 100, 101) \\ E_{10} & = (011, 001, 110, 100, 111, 010, 000, 101) & E_{11} & = (000, 011, 001, 101, 110, 100, 111, 010) \end{array}$$

   (a) Consider the ECB encryption mode studied in class. Let $K = 10, M_1 = 011101$, and $M_2 = 010101$. Compute the values of C_1 and C_2 resulting from encrypting M_1 and M_2, respectively, with ECB using the key K. Show your work. Be precise.

   (b) Consider the CBCC encryption mode studied in class. Let $K = 00, M_1 = 101010$, and $M_2 = 110100$. Compute C_1 and C_2 resulting from encrypting M_1 and M_2, respectively, with CBCC using the key K. Show your work. Be precise.

   (c) Consider CBC$ encryption mode studied in class. Let $K = 01, M_1 = 100001$, and $M_2 = 101000$. Compute C_1 and C_2 resulting from encrypting M_1 and M_2, respectively, with CBC$ using the key K and IV = 011 for M_1 and IV=010 for M_2. Show your work. Be precise.

   (d) Consider CTRC encryption mode studied in class. Let $K = 11, M_1 = 110101$, and $M_2 = 001100$. Compute C_1 and C_2 resulting from encrypting M_1 and M_2, respectively, with CTRC using the key K. Show your work. Be precise.

   (e) Consider CBCC encryption mode studied in class. Let $K = 10, C_1 = 110011001$, and $C_2 = 010101100$. Compute M_1 and M_2 resulting from decrypting C_1 and C_2 with CBCC using the key K. Show your work. Be precise.

   (f) Consider CTR$ encryption mode studied in class. Let $K = 00, C_1 = 011101011$, and $C_2 = 010101010$. Compute M_1 and M_2 resulting from decrypting C_1 and C_2 with CTR$ using the key K. Show your work. Be precise.

3. For this problem, we consider how TLS 1.0 uses CBC, in particular, how the initialization vector (IV) is computed according to RFC 2246: *The TLS Protocol Version 1.0*. The following paragraph from page 19 of the standard describes how implementors are supposed to compute the IV.

> Note: With block ciphers in CBC mode (Cipher Block Chaining) the initialization vector (IV) for the first record is generated with the other keys and secrets when the security parameters are set. The IV for subsequent records is the last ciphertext block from the previous record.

   Here, for simplicity, we assume that the first IV is simply a bitstring chosen uniform randomly from the set of all bitstrings of length equal to the block length of the underlying block cipher.

   Let $E : \{0,1\}^{256} \times \{0,1\}^{256} \to \{0,1\}^{256}$ be a block cipher. Consider a symmetric encryption scheme $\mathcal{SE} = (\mathsf{KG}, \mathcal{E}, \mathcal{D})$ with a key generation algorithm KG that outputs a 256-bit string drawn uniformly at random from $\{0,1\}^{256}$ and an encryption algorithm $\mathcal{E}$ that works as described below.

   Algorithm $\mathcal{E}(K, M)$
   If ($|M| = 0$) or ($|M| \bmod 256 \neq 0$) then return $\perp$
   Parse M as 256-bit blocks $M[1] \dots M[m]$
   static $IV \xleftarrow{\$} \{0,1\}^{256}$

$C[0] \leftarrow IV$
For $i = 1$ to m do $C[i] \leftarrow E_K(M[i] \oplus C[i-1])$
$IV \leftarrow C[m]$
Return $C[0] \dots C[m]$

(a) What is the ciphertext expansion for this encryption scheme in bits?

(b) Write in pseudocode the decryption algorithm that would make the triple $(\mathsf{KG}, \mathcal{E}, \mathcal{D})$ form a symmetric encryption scheme $\mathcal{SE}$ satisfying the correctness condition for symmetric encryption schemes.

(c) Suppose E is a block cipher secure under PRP-CCA. Is $\mathcal{SE}$ a symmetric encryption scheme secure under IND-CPA?

(d) Prove your answer to the previous question. Specifically, if your answer is yes, provide a complete reduction-based proof. If your answer is no, explicitly provide pseudocode for the attacker. Your proof must contain four parts: (1) the description of the idea behind the reduction or the attack, (2) the pseudocode for the reduction or the attacker, (3) the analysis of the advantage of the attacker, and (4), the attacker's resource usage. For an attack, the smaller the resource usage required and the larger the advantage, the better.

4. Let $E : \{0,1\}^{256} \times \{0,1\}^{256} \to \{0,1\}^{256}$ be a block cipher. Consider a symmetric encryption scheme $\mathcal{SE} = (\mathsf{KG}, \mathcal{E}, \mathcal{D})$ with a key generation algorithm KG that outputs a 256-bit string drawn uniformly at random from $\{0,1\}^{256}$ and an encryption algorithm $\mathcal{E}$ that works as described below. Note that in the pseudocode, you can assume automatic type conversion between integers and their binary representation as bitstrings.

Algorithm $\mathcal{E}(K, M)$
If $(|M| = 0)$ or $(|M| \bmod 256 \neq 0)$ then return $\perp$
Parse M as 256-bit blocks $M[1] \dots M[m]$
static $ctr \leftarrow 0$
$C[0] \leftarrow ctr$; $ctr \leftarrow ctr + 1$
For $i = 1$ to m do $C[i] \leftarrow E_K(C[0] + i - 1) \oplus M[i]$
Return $C[0] \dots C[m]$

(a) Explain the similarity and differences between this type of encryption and CTRC mode studied in class.

(b) What is the ciphertext expansion for this encryption scheme in bits?

(c) Write in pseudocode the decryption algorithm that would make the triple $(\mathsf{KG}, \mathcal{E}, \mathcal{D})$ form a symmetric encryption scheme $\mathcal{SE}$ satisfying the correctness condition for symmetric encryption schemes.

(d) Suppose E is a block cipher secure under PRP-CCA. Is $\mathcal{SE}$ a symmetric encryption scheme secure under IND-CPA?

(e) Prove your answer to the previous question. Specifically, if your answer is yes, provide a complete reduction-based proof. If your answer is no, explicitly provide pseudocode for the attacker. Your proof must contain four parts: (1) the description of the idea behind the reduction or the attack, (2) the pseudocode for the reduction or the attacker, (3) the analysis of the advantage of the attacker, and (4), the attacker's resource usage. For an attack, the smaller the resource usage required and the larger the advantage, the better.

5. Consider the following security definition for symmetric encryption schemes.

Let $\mathsf{SE} = (\mathsf{KG}, \mathcal{E}, \mathcal{D})$ be a symmetric encryption scheme, and let A be an adversary with access to an oracle. We define the following subroutines, experiment, and advantage function.

Subroutine $\texttt{Initialize}(w)$ $b \leftarrow w$; $K \xleftarrow{\$} \mathsf{KG}$ Subroutine $\texttt{Enc}(M_0, M_1)$ If $\lvert M_0\rvert \neq \lvert M_1\rvert$ then return $\perp$ Return $\mathcal{E}_K(M_b)$	Experiment $\mathbf{Exp}^{\text{ind-cpa-w}}_{\mathsf{SE}}(A)$ $\texttt{Initialize}(w)$ $d \xleftarrow{\$} A^{\texttt{Enc}}$ Return d

We define the *ind-cpa* advantage* of an adversary A mounting a chosen-plaintext attack against SE as

$$\mathbf{Adv}^{\text{ind-cpa*}}_{\mathsf{SE}}(A) = \Pr\left[\,\mathbf{Exp}^{\text{ind-cpa-1}}_{\mathsf{SE}}(A) \Rightarrow 1\,\right] - \Pr\left[\,\mathbf{Exp}^{\text{ind-cpa-0}}_{\mathsf{SE}}(A) \Rightarrow 1\,\right] .$$

Recall the definition of $\mathbf{Adv}^{\text{ind-cpa}}$ defined in the textbook and studied in class. Prove that, for all SE and A,

$$\mathbf{Adv}^{\text{ind-cpa*}}_{\mathsf{SE}}(A) = \mathbf{Adv}^{\text{ind-cpa}}_{\mathsf{SE}}(A) .$$

6. Consider the following security definition for symmetric encryption schemes.

Let $\mathsf{SE} = (\mathsf{KG}, \mathcal{E}, \mathcal{D})$ be a symmetric encryption scheme, and let A be an adversary with access to an oracle. We define the following subroutines, experiment, and advantage function.

Subroutine $\texttt{Initialize}(w)$ $b \leftarrow w$; $K \xleftarrow{\$} \mathsf{KG}$ Subroutine $\texttt{Enc}(M)$ If $b = 0$ then $M \xleftarrow{\$} \{0,1\}^{\lvert M\rvert}$ Return $\mathcal{E}_K(M)$	Experiment $\mathbf{Exp}^{\text{ror-ind-cpa-w}}_{\mathsf{SE}}(A)$ $\texttt{Initialize}(w)$ $d \xleftarrow{\$} A^{\texttt{Enc}}$ Return d

We define the *ror (real-or-random) ind-cpa advantage* of an adversary A mounting a chosen-plaintext attack against SE as

$$\mathbf{Adv}^{\text{ror-ind-cpa}}_{\mathsf{SE}}(A) = \Pr\left[\,\mathbf{Exp}^{\text{ror-ind-cpa-1}}_{\mathsf{SE}}(A) \Rightarrow 1\,\right] - \Pr\left[\,\mathbf{Exp}^{\text{ror-ind-cpa-0}}_{\mathsf{SE}}(A) \Rightarrow 1\,\right] .$$

Recall the definition of $\mathbf{Adv}^{\text{ind-cpa}}$ defined in the textbook and studied in class.

(a) Prove that, for all SE and adversary A, there exists an adversary B using comparable resources to A such that

$$\mathbf{Adv}^{\text{ror-ind-cpa}}_{\mathsf{SE}}(A) = \mathbf{Adv}^{\text{ind-cpa}}_{\mathsf{SE}}(B) .$$

(b) Prove that, for all SE and adversary B, there exists an adversary A using comparable resources to B such that

$$\mathbf{Adv}^{\text{ind-cpa}}_{\mathsf{SE}}(B) \leq 2 \cdot \mathbf{Adv}^{\text{ror-ind-cpa}}_{\mathsf{SE}}(A) .$$