Sample Solutions for Problem Set 2

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

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)

   (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.

> **Solution:** Encrypting M_1 then M_2, respectively, using the key $K = 10$, we obtain
>
> $$C_1 = E_{10}(011)\|E_{10}(101) = 100010 \text{ and}$$
> $$C_2 = E_{10}(010)\|E_{10}(101) = 110010\ .$$

   (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.

> **Solution:** Encrypting M_1 then M_2, respectively, using the key $K = 00$, we obtain
>
> $$\begin{aligned} C_1 &= 000\|E_{00}(000 \oplus 101)\|E_{00}(E_{00}(000 \oplus 101) \oplus 010) \\ &= 000\|E_{00}(101)\|E_{00}(E_{00}(101) \oplus 010) \\ &= 000\|111\|E_{00}(111 \oplus 010) \\ &= 000\|111\|E_{00}(101) \\ &= 000111111 \text{ and} \\ C_2 &= 001\|E_{00}(001 \oplus 110)\|E_{00}(E_{00}(001 \oplus 110) \oplus 100) \\ &= 001\|E_{00}(111)\|E_{00}(E_{00}(111) \oplus 100) \\ &= 001\|001\|E_{00}(001 \oplus 100) \\ &= 001\|001\|E_{00}(101) \\ &= 001001111\ . \end{aligned}$$

   (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.

Solution: Encrypting M_1 then M_2, respectively, using the key $K = 01$, we obtain

$$\begin{aligned}
C_1 &= 011 \| E_{01}(011 \oplus 100) \| E_{01}(E_{01}(011 \oplus 100) \oplus 001) \\
&= 011 \| E_{01}(111) \| E_{01}(E_{01}(111) \oplus 001) \\
&= 011 \| 101 \| E_{01}(101 \oplus 001) \\
&= 011 \| 101 \| E_{01}(100) \\
&= 011101110 \text{ and} \\
C_2 &= 010 \| E_{01}(010 \oplus 101) \| E_{01}(E_{01}(010 \oplus 101) \oplus 000) \\
&= 010 \| E_{01}(111) \| E_{01}(E_{01}(111) \oplus 000) \\
&= 010 \| 101 \| E_{01}(101 \oplus 000) \\
&= 010 \| 101 \| E_{01}(101) \\
&= 010101011 \, .
\end{aligned}$$

(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.

Solution: We assume that the counter starts at 0 for the encipherment of the first block of the first message. Encrypting M_1 then M_2, respectively, using the key $K = 11$, we obtain

$$\begin{aligned}
C_1 &= 000 \| E_{11}(000) \oplus 110 \| E_{11}(001) \oplus 101 \\
&= 000 \| 000 \oplus 110 \| 011 \oplus 101 \\
&= 000110110 \text{ and} \\
C_2 &= 010 \| E_{11}(010) \oplus 001 \| E_{11}(011) \oplus 100 \\
&= 010 \| 001 \oplus 001 \| 101 \oplus 100 \\
&= 010000001 \, .
\end{aligned}$$

(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.

Solution: We assume that the counter starts at 0 for the IV. Encrypting M_1 then M_2, respectively, using the key $K = 10$, we obtain

$$\begin{aligned}
C_1 &= E_{10}^{-1}(011) \oplus 110 \parallel E_{10}^{-1}(001) \oplus 011 \\
&= 000 \oplus 110 \parallel 001 \oplus 011 \\
&= 110010 \text{ and} \\
C_2 &= E_{10}^{-1}(101) \oplus 010 \parallel E_{10}^{-1}(100) \oplus 101 \\
&= 111 \oplus 010 \parallel 011 \oplus 101 \\
&= 101110 \, .
\end{aligned}$$

(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.

Solution: Encrypting M_1 then M_2, respectively, using the key $K = 00$, we obtain

$$\begin{aligned} M_1 &= E_{00}(011) \oplus 101 \parallel E_{00}(100) \oplus 011 \\ &= 000 \oplus 101 \parallel 101 \oplus 011 \\ &= 101110 \text{ and} \\ M_2 &= E_{00}(010) \oplus 101 \parallel E_{00}(011) \oplus 010 \\ &= 010 \oplus 101 \parallel 000 \oplus 010 \\ &= 111010 \,. \end{aligned}$$

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?

Solution: The ciphertext expansion comes from the first ciphertext block. So the expansion is 256 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.

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

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

Solution: No.

(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.

Solution:

Idea: First, we ask one query to let the encryption algorithm set the initial IV. Then, we exploit the fact that, from this point on, we know the values of all the IVs that the encryption algorithm will use to encrypt messages. To choose the second message, we use the known IV to force the input to the block cipher to (1) repeat if we have the left-encrypting oracle and (2) to not repeat if we have the right-encrypting oracle. Finally, if the resulting ciphertext is what we have seen before, then we know that we have the left-encrypting oracle. Otherwise, we know that we have the right-encrypting oracle.

Pseudocode for the adversary:
Adversary $A^{\texttt{Enc}}$
$C \xleftarrow{\$} \texttt{Enc}(0^{256}, 0^{256})$
Parse C as 256-bit blocks $C[0]C[1]$
$C' \xleftarrow{\$} \texttt{Enc}(C[0] \oplus C[1], C[0] \oplus C[1] \oplus 1^{256})$
Parse C' as 256-bit blocks $C'[0]C'[1]$
If $C'[1] = C[1]$ then return 0 else return 1

Analysis: Let SE be the scheme in question. We are interested in the quantity $\mathbf{Adv}^{\text{ind-cpa}}_{\mathsf{SE}}(A)$.

Case 1: Let `Enc` be the left oracle. Thus,

$$\begin{aligned} C[1] &= E_K(C[0] \oplus 0^{256}) \\ &= E_K(C[0]), \text{ and} \\ C'[1] &= E_K(C[1] \oplus (C[0] \oplus C[1])) \\ &= E_K(C[0]) \end{aligned}$$

where the third line follows from the fact that $C[1]$ is used as the IV to encrypt the second message. Therefore, $C'[1] = C[1]$, and A returns 0. So, A always answers correctly.

Case 2: Let `Enc` be the right oracle. Thus,

$$\begin{aligned} C[1] &= E_K(C[0] \oplus 0^{256}) \\ &= E_K(C[0]), \text{ and} \\ C'[1] &= E_K(C[1] \oplus (C[0] \oplus C[1] \oplus 1^{256})) \\ &= E_K(C[0] \oplus 1^{256}) \end{aligned}$$

Since E_K is a permutation, $C'[1] \neq C[1]$. Thus, A returns 1, and A always answers correctly.

Let b be the bit that the challenger uses to determine whether to encrypt the left message

($b = 0$) or the right message ($b = 1$). We compute the advantage of A as follows:

$$\begin{aligned}
\mathbf{Adv}^{\text{ind-cpa}}_{\mathsf{SE}}(A) &= 2 \cdot \Pr\left[\, \mathbf{Exp}^{\text{ind-cpa}}_{\mathsf{SE}}(A) \Rightarrow \mathbf{T} \,\right] - 1 \\
&= 2 \cdot (\Pr\left[\, \mathbf{Exp}^{\text{ind-cpa}}_{\mathsf{SE}}(A) \Rightarrow \mathbf{T} \mid b = 0 \,\right] \cdot \Pr[\, b = 0 \,] \\
&\quad + \Pr\left[\, \mathbf{Exp}^{\text{ind-cpa}}_{\mathsf{SE}}(A) \Rightarrow \mathbf{T} \mid b = 1 \,\right] \cdot \Pr[\, b = 1 \,]) - 1 \\
&= 2 \cdot \left(\Pr\left[\, \mathbf{Exp}^{\text{ind-cpa}}_{\mathsf{SE}}(A) \Rightarrow \mathbf{T} \mid b = 0 \,\right] \cdot \frac{1}{2} + \Pr\left[\, \mathbf{Exp}^{\text{ind-cpa}}_{\mathsf{SE}}(A) \Rightarrow \mathbf{T} \mid b = 1 \,\right] \cdot \frac{1}{2}\right) - 1 \\
&= \Pr\left[\, \mathbf{Exp}^{\text{ind-cpa}}_{\mathsf{SE}}(A) \Rightarrow \mathbf{T} \mid b = 0 \,\right] + \Pr\left[\, \mathbf{Exp}^{\text{ind-cpa}}_{\mathsf{SE}}(A) \Rightarrow \mathbf{T} \mid b = 1 \,\right] - 1 \\
&= 1 + 1 - 1 \\
&= 1
\end{aligned}$$

where the second to last line was due to the analysis results for Cases 1 and 2 above.

Resource usage: From the pseudocode, we see that A uses 2 encryption queries totalling 512 bits. (Recall that we only count the number of bits that get encrypted by the oracle.) The running time of A is $O(1)$ plus the time it takes to complete two encryption oracle queries.

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 $M[1] \ldots M[m]$
  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 $C[0] \ldots C[m]$

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

Solution: The similarity is that it is a counter mode encryption scheme that keeps track of the counter across encryption calls. The difference is that the encryption algorithm for this scheme increments the counter value by 1 *per message* that gets encrypted, rather than *per block* as done in the CTRC mode studied in class.

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

Solution: The ciphertext expansion comes from the first ciphertext block. So the expansion is 256 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.

Solution:

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

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

Solution: No.

(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.

Solution:

Idea: Since the counter value is incremented per message, rather than per block of the input message, we first submit a 2-block message containing only zeros to obtain the encipherment of the binary representation of the integer 1. Since we know that, for the encryption of the second message, the encryption algorithm will use 1 as the counter, we know that it will xor the same encipherment result to the message of our own choosing. Consequently, we know exactly what the outcome should be. So we can submit distinct messages for the second encryption query and tell the difference between the left-encrypting and right-encrypting oracles by comparing the ciphertext output to our expectation.

Pseudocode for the adversary: We assume that the counter starts at 0 for the encipherment of the first block of the first message.

Adversary $A^{\mathtt{Enc}}$
  $C \xleftarrow{\$} \mathtt{Enc}(0^{512}, 0^{512})$
  $C' \xleftarrow{\$} \mathtt{Enc}(0^{256}, 1^{256})$
  Parse C as 256-bit blocks $C[0]C[1]C[2]$
  Parse C' as 256-bit blocks $C'[0]C'[1]$
  If $C[2] = C'[1]$ then return 0 else return 1

Analysis: Let SE be the scheme in question. We are interested in the quantity $\mathbf{Adv}^{\text{ind-cpa}}_{\mathsf{SE}}(A)$.

Case 1: Let $\mathtt{Enc}$ be the left oracle. Thus,

$$\begin{aligned} C[2] &= E_K(0^{255}1) \oplus 0^{256} \\ &= E_K(0^{255}1), \text{ and} \\ C'[1] &= E_K(0^{255}1) \oplus 0^{256} \\ &= E_K(0^{255}1) \end{aligned}$$

where the third line follows follows from the fact that, for the encryption of the second message, namely 0^{256}, the counter starts at 1.

Therefore, $C[2] = C'[1]$, and A returns 0. So, A always answers correctly.

Case 2: Let `Enc` be the right oracle. Thus,

$$\begin{aligned} C[2] &= E_K(0^{255}1) \oplus 0^{256} \\ &= E_K(0^{255}1), \text{ and} \\ C'[1] &= E_K(0^{255}1) \oplus 1^{256} \end{aligned}$$

where the third line follows follows from the fact that, for the encryption of the second message, namely 1^{256}, the counter starts at 1.

Clearly, $C[2] \neq C'[1]$. Thus, A returns 1, and A always answers correctly.

Let b be the bit that the challenger uses to determine whether to encrypt the left message ($b = 0$) or the right message ($b = 1$). We compute the advantage of A as follows:

$$\begin{aligned} \mathbf{Adv}^{\text{ind-cpa}}_{\mathsf{SE}}(A) &= 2 \cdot \Pr\left[\, \mathbf{Exp}^{\text{ind-cpa}}_{\mathsf{SE}}(A) \Rightarrow \mathbf{T} \,\right] - 1 \\ &= 2 \cdot (\Pr\left[\, \mathbf{Exp}^{\text{ind-cpa}}_{\mathsf{SE}}(A) \Rightarrow \mathbf{T} \mid b = 0 \,\right] \cdot \Pr[\, b = 0 \,] \\ &\quad + \Pr\left[\, \mathbf{Exp}^{\text{ind-cpa}}_{\mathsf{SE}}(A) \Rightarrow \mathbf{T} \mid b = 1 \,\right] \cdot \Pr[\, b = 1 \,]) - 1 \\ &= 2 \cdot \left(\Pr\left[\, \mathbf{Exp}^{\text{ind-cpa}}_{\mathsf{SE}}(A) \Rightarrow \mathbf{T} \mid b = 0 \,\right] \cdot \frac{1}{2} + \Pr\left[\, \mathbf{Exp}^{\text{ind-cpa}}_{\mathsf{SE}}(A) \Rightarrow \mathbf{T} \mid b = 1 \,\right] \cdot \frac{1}{2} \right) - 1 \\ &= \Pr\left[\, \mathbf{Exp}^{\text{ind-cpa}}_{\mathsf{SE}}(A) \Rightarrow \mathbf{T} \mid b = 0 \,\right] + \Pr\left[\, \mathbf{Exp}^{\text{ind-cpa}}_{\mathsf{SE}}(A) \Rightarrow \mathbf{T} \mid b = 1 \,\right] - 1 \\ &= 1 + 1 - 1 \\ &= 1 \end{aligned}$$

where the second to last line was due to the analysis results for Cases 1 and 2 above.

Resource usage: From the pseudocode, we see that A uses 2 encryption queries totalling 768 bits. (Recall that we only count the number of bits that get encrypted by the oracle.) The running time of A is $O(1)$ plus the time it takes to complete two encryption oracle queries.

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 `Initialize`(w)
  $b \leftarrow w$; $K \xleftarrow{\$} \mathsf{KG}$
 	
Subroutine `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 $\mathbf{Exp}^{\text{ind-cpa-w}}_{\mathsf{SE}}(A)$
	
	  `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,

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

Solution: Recall the definition of the advantage of an adversary in the IND-CPA game as studied in class:

$$\mathbf{Adv}^{\text{ind-cpa}}_{\mathsf{SE}}(A) = 2 \cdot \Pr\left[\, \mathbf{Exp}^{\text{ind-cpa}}_{\mathsf{SE}}(A) \Rightarrow \mathbf{T} \,\right] - 1 \; . \tag{1}$$

Consider the expression $\Pr\left[\, \mathbf{Exp}^{\text{ind-cpa}}_{\mathsf{SE}}(A) \Rightarrow \mathbf{T} \,\right]$. Recognizing that the challenger picks the bit b for the experiment $\mathbf{Exp}^{\text{ind-cpa}}_{\mathsf{SE}}(A)$ uniform randomly and applying Bayes' theorem, we obtain

$$\begin{aligned}\Pr\left[\, \mathbf{Exp}^{\text{ind-cpa}}_{\mathsf{SE}}(A) \Rightarrow \mathbf{T} \,\right] &= \Pr\left[\, \mathbf{Exp}^{\text{ind-cpa}}_{\mathsf{SE}}(A) \Rightarrow \mathbf{T} \mid b = 1 \,\right] \cdot \frac{1}{2} \\ &\quad + \Pr\left[\, \mathbf{Exp}^{\text{ind-cpa}}_{\mathsf{SE}}(A) \Rightarrow \mathbf{T} \mid b = 0 \,\right] \cdot \frac{1}{2} \; .\end{aligned}$$

Now, since

$$\begin{aligned}\Pr\left[\, \mathbf{Exp}^{\text{ind-cpa}}_{\mathsf{SE}}(A) \Rightarrow \mathbf{T} \mid b = 1 \,\right] &= \Pr\left[\, \mathbf{Exp}^{\text{ind-cpa-1}}_{\mathsf{SE}}(A) \Rightarrow 1 \,\right] \text{ and} \\ \Pr\left[\, \mathbf{Exp}^{\text{ind-cpa}}_{\mathsf{SE}}(A) \Rightarrow \mathbf{T} \mid b = 0 \,\right] &= 1 - \Pr\left[\, \mathbf{Exp}^{\text{ind-cpa-0}}_{\mathsf{SE}}(A) \Rightarrow 1 \,\right] \; ,\end{aligned}$$

we have

$$\Pr\left[\, \mathbf{Exp}^{\text{ind-cpa}}_{\mathsf{SE}}(A) \Rightarrow \mathbf{T} \,\right] = \Pr\left[\, \mathbf{Exp}^{\text{ind-cpa-1}}_{\mathsf{SE}}(A) \Rightarrow 1 \,\right] \cdot \frac{1}{2} + (1 - \Pr\left[\, \mathbf{Exp}^{\text{ind-cpa-0}}_{\mathsf{SE}}(A) \Rightarrow 1 \,\right]) \cdot \frac{1}{2} \; . \tag{2}$$

Substituting the quantity in Equation (2) into Equation (1), we obtain

$$\begin{aligned}\mathbf{Adv}^{\text{ind-cpa}}_{\mathsf{SE}}(A) &= 2 \cdot \left(\Pr\left[\, \mathbf{Exp}^{\text{ind-cpa-1}}_{\mathsf{SE}}(A) \Rightarrow 1 \,\right] \cdot \frac{1}{2} + (1 - \Pr\left[\, \mathbf{Exp}^{\text{ind-cpa-0}}_{\mathsf{SE}}(A) \Rightarrow 1 \,\right]) \cdot \frac{1}{2} \right) - 1 \\ &= \Pr\left[\, \mathbf{Exp}^{\text{ind-cpa-1}}_{\mathsf{SE}}(A) \Rightarrow 1 \,\right] - \Pr\left[\, \mathbf{Exp}^{\text{ind-cpa-0}}_{\mathsf{SE}}(A) \Rightarrow 1 \,\right] \\ &= \mathbf{Adv}^{\text{ind-cpa*}}_{\mathsf{SE}}(A) \text{ as desired.}\end{aligned}$$

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

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

Solution: Let A be an adversary. Let Games $G0$ and $G1$ be the following games:

Game $G0$:
$K \xleftarrow{\$} \mathsf{KG}$
Run A answering its queries as follows:
Upon receiving a query $\mathtt{Enc}(M)$ from A, do
$M \xleftarrow{\$} \{0,1\}^{|M|}$
Send $\mathcal{E}_K(M)$ to A
Until A stops and return d
Return d

Game $G1$:
$K \xleftarrow{\$} \mathsf{KG}$
Run A answering its queries as follows:
Upon receiving a query $\mathtt{Enc}(M)$ from A, do
Send $\mathcal{E}_K(M)$ to A
Until A stops and returns d
Return d

Notice that

$$\mathbf{Adv}^{\text{ror-ind-cpa}}_{\mathsf{SE}}(A) = \Pr\left[\, G1(A) \Rightarrow 1 \,\right] - \Pr\left[\, G0(A) \Rightarrow 1 \,\right] \ . \tag{3}$$

We construct an adversary B with access to an oracle $\mathtt{Enc}(\cdot,\cdot)$ and adversary A as follows:

Adversary $B^{\mathtt{Enc}}$:
Run A answering its queries $\mathtt{Enc}(M)$ as follows:
$M_0 \xleftarrow{\$} \{0,1\}^{|M|}$
$C \xleftarrow{\$} \mathtt{Enc}(M_0, M)$
Send C to A
Until A stops and returns d
Return d

When B's oracle is a right-encrypting one, the environment in which B simulates A is exactly the same as that of $\mathbf{Exp}^{\text{ror-ind-cpa-1}}_{\mathsf{SE}}(A)$, which is the same as $G1$. Similarly, when B's oracle is a left-encrypting one, the environment in which B simulates A is exactly the same as that of $\mathbf{Exp}^{\text{ror-ind-cpa-0}}_{\mathsf{SE}}(A)$, which is the same as $G0$. Thus, we have that

$$\Pr\left[\, \mathbf{Exp}^{\text{ind-cpa-1}}_{\mathsf{SE}}(B) \Rightarrow 1 \,\right] = \Pr\left[\, G1(A) \Rightarrow 1 \,\right] \qquad \text{and} \tag{4}$$

$$\Pr\left[\, \mathbf{Exp}^{\text{ind-cpa-0}}_{\mathsf{SE}}(B) \Rightarrow 1 \,\right] = \Pr\left[\, G0(A) \Rightarrow 1 \,\right] \ . \tag{5}$$

Therefore, substituting Equations (4) and (5) into Equation (6), we get

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

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

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

Solution: Let B be an adversary. Let Games $G0$ and $G1$ be the following games:

Game $G0$:
$x \xleftarrow{\$} \{0,1\}$; $K \xleftarrow{\$} \mathsf{KG}$
Run B answering its queries as follows:
Upon receiving a query $\mathtt{Enc}(M_0, M_1)$ from B, do
Send $\mathcal{E}_K(M_x)$ to B
Until B stops and return d
If $x = d$, then return 1 else return 0

Game $G1$:
$x \xleftarrow{\$} \{0,1\}$; $K \xleftarrow{\$} \mathsf{KG}$
Run B answering its queries as follows:
Upon receiving a query $\mathtt{Enc}(M_0, M_1)$ from B, do
$M_x \xleftarrow{\$} \{0,1\}^{|M|}$
Send $\mathcal{E}_K(M_x)$ to B
Until B stops and returns d
If $x = d$, then return 1 else return 0

Additionally, we define an adversary A with access to an oracle $\mathtt{Enc}(\cdot)$ and B as follows:

Adversary $A^{\mathtt{Enc}}$:
$x \xleftarrow{\$} \{0,1\}$
Run B answering its queries $\mathtt{Enc}(M_0, M_1)$ as follows:
$C \xleftarrow{\$} \mathtt{Enc}(M_x)$
Send C to B
Until B stops and returns d
If $x = d$, then return 1 else return 0

Recall the definition of advantage function in the IND-CPA game:

$$\mathbf{Adv}^{\text{ind-cpa}}_{\mathsf{SE}}(B) = 2 \cdot \Pr\left[\, \mathbf{Exp}^{\text{ind-cpa}}_{\mathsf{SE}}(B) \Rightarrow \mathbf{T} \,\right] - 1 \,. \tag{6}$$

We focus on the probability term on the right and obtain the following derivation:

$$\begin{aligned}
\Pr\left[\, \mathbf{Exp}^{\text{ind-cpa}}_{\mathsf{SE}}(B) \Rightarrow \mathbf{T} \,\right] &= \Pr\left[\, G0(B) \Rightarrow 1 \,\right] && (7)\\
&= \Pr\left[\, G0(B) \Rightarrow 1 \,\right] - \Pr\left[\, G1(B) \Rightarrow 1 \,\right] + \Pr\left[\, G1(B) \Rightarrow 1 \,\right] \\
&= \Pr\left[\, \mathbf{Exp}^{\text{ror-ind-cpa-1}}_{\mathsf{SE}}(A) \Rightarrow 1 \,\right] - \Pr\left[\, \mathbf{Exp}^{\text{ror-ind-cpa-0}}_{\mathsf{SE}}(A) \Rightarrow 1 \,\right] \\
&\quad + \Pr\left[\, G1(B) \Rightarrow 1 \,\right] && (8)\\
&\leq \Pr\left[\, \mathbf{Exp}^{\text{ror-ind-cpa-1}}_{\mathsf{SE}}(A) \Rightarrow 1 \,\right] - \Pr\left[\, \mathbf{Exp}^{\text{ror-ind-cpa-0}}_{\mathsf{SE}}(A) \Rightarrow 1 \,\right] + \frac{1}{2} && (9)\\
&= \mathbf{Adv}^{\text{ror-ind-cpa}}_{\mathsf{SE}}(A) + \frac{1}{2} \,. && (10)
\end{aligned}$$

We justify some of the equations above in turn. Equation (7) follows because $G0$ is essentially the definition of the IND-CPA game. Equation (8) follows because, in A's simulation of B,

(a) if A's oracle is a real-message-encrypting one, the environment in which A simulates B is the same as that of $G0$, and

(b) if A's oracle is a random-message-encrypting one, the environment in which A simulates B is the same as that of $G1$.

Thus, (a) implies that the probability that B guesses the bit x correctly in $G0(B)$ is the same as the probability that B guesses the bit x correctly in A's simulation of B when A's oracle is a real-message-encrypting oracle. According to A's pseudocode, this probability is the same as the probability that A returns 1. Similarly, (b) implies that the probability that B guesses the bit x correctly in $G1(B)$ is the same as the probability that B guesses the bit x correctly in A's simulation of B when A's oracle is a random-message-encrypting oracle. According to A's pseudocode, this probability is the same as the probability that A returns 1. Thus, Equation (8) follows. Inequality (9) follows because, in Game $G1$, B's queries and the corresponding answers to the queries are independent from each other. Therefore, the probability that B's output is correct is at most $\frac{1}{2}$. Finally, Equation (10) follows by definition of the ROR IND-CPA game.

Substituting Equation (10) into Equation (6), we obtain

$$\begin{aligned}
\mathbf{Adv}^{\text{ind-cpa}}_{\mathsf{SE}}(B) &\leq 2 \cdot \left(\mathbf{Adv}^{\text{ror-ind-cpa}}_{\mathsf{SE}}(A) + \frac{1}{2} \right) - 1 \\
&= 2 \cdot \mathbf{Adv}^{\text{ror-ind-cpa}}_{\mathsf{SE}}(A) \,.
\end{aligned}$$