Solutions for Assignment 7

1. Choose the correct option(s) from the following:

   a. If an encryption scheme is an authenticated encryption scheme, then it is also CPA-secure

   b. If an encryption scheme is CPA-secure, then it is also an authenticated encryption scheme

   c. A secure authenticated encryption scheme cannot be constructed using a malleable encryption scheme

   d. A secure authenticated encryption scheme is necessarily CCA secure

   A CPA-secure encryption scheme need not satisfy ciphertext integrity and hence need not be an authenticated encryption scheme. An authenticated encryption scheme is always CPA-secure. The third statement is false, as we can generically combine *any* CPA-secure cipher (which could be malleable and hence not CCA-secure) and a secure MAC to get an authenticated encryption scheme. The last statement is true, as it follows from the definition of AE. So the answers are **a** and **d**.

2. Select the incorrect option(s):

   a. To break the security of a cryptographic construction which is provably-secure in the ROM model, one must discover a weakness in the actual hash function

   b. There doesn't exist any ROM based crypto primitive that is efficient and highly secure

   c. In the ROM model, unique queries are always answered with unique answers

   d. There are schemes secure in the RO model, but insecure when using any real-world hash function

   Statements **b, c** are incorrect. Hence, the correct answers are **b, c**. The second statement is false, as there are ROM based crypto primitives that are efficient and highly secure. The third statement is false, as each query is answered independently, but not uniquely.

3. Let $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ be a symmetric-key encryption scheme with message-space $\mathcal{M}$. We construct a new symmetric-key encryption scheme $\Pi' = (\text{Gen}', \text{Enc}', \text{Dec}')$ for message space $\mathcal{M}^2$ as follows: the key-generation algorithm Gen' outputs $k = (k_0, k_1)$ as the key, where Gen' invokes two independent instances of Gen, which outputs k_0 and k_1 respectively. To encrypt a plaintext $(m_0, m_1) \in \mathcal{M}^2$, the encryption algorithm $\text{Enc}'_k(m_0, m_1)$ outputs (c_0, c_1) as the ciphertext, where $c_0 = \text{Enc}_{k_0}(m_0)$ and $c_1 = \text{Enc}_{k_1}(m_1)$. The decryption algorithm $\text{Dec}'_k(c_0, c_1)$ outputs $\text{Dec}_{k_0}(c_0), \text{Dec}_{k_1}(c_1)$.

   a. The scheme Π' provides ciphertext integrity

   b. If Π is multi-message COA-secure then Π' is also multi-message COA-secure

   c. If Π is CCA-secure then Π' is also CCA-secure

   d. If Π is CPA-secure then Π' is also CPA-secure

   The scheme Π' does not have ciphertext integrity, as an adversary can easily produce a valid ciphertext from the ciphertext space of Π' and hence the scheme is not an authenticated encryption scheme. The scheme is also not CCA-secure. A CCA adversary can submit the challenge plaintexts $M_0 = (m_0, m_1)$ and $M_1 = (m'_0, m'_1)$, where $m_0 \neq m_1 \neq m'_0 \neq m'_1$. On receiving the challenge ciphertext $c^\star = (c^\star_0, c^\star_1)$, the adversary can ask for the decryption oracle service for the modified ciphertext $(c^\star_0, c_1)$, where c_1 is some bit-string, different from $c^\star_1$. In response, the oracle will either return $(m_0, \star)$ or $(m_1, \star)$ and the adversary can easily identify whether $c^\star$ is an encryption of M_0 or M_1. However, the scheme Π' will be CPA-secure (and hence COA-secure), if Π is CPA-secure (COA-secure). So the answers are **b** and **d**.

4. Choose the correct combination for Commitment Schemes:

1. Receiver	i. Hiding Property
2. Corrupt sender, honest receiver	ii. Provides opening information
3. Honest sender. corrupt receiver	iii. Accept or reject data m
4. Sender	iv. Binding property

a. 1-iii, 2-iv, 3-i, 4-ii

b. 1-ii, 2-iv, 3-i, 4-iii

c. 1-i, 2-iv, 3-ii, 4-iii

d. 1-iii, 2-i, 3-iv, 4-ii

The correct answer is **a**. In a commitment scheme, the sender provides the opening information during the opening phase. For an honest sender and a corrupt receiver, we need the hiding property to hold during the commit phase. For the corrupt sender and honest receiver, we need the binding property to hold during the opening phase. And finally, based on whether the commitment has been opened correctly or not, receiver accepts or rejects the data.

5. Let $(E(k,m), D(k,c))$, for key $k \in \{0,1\}^n$ chosen at random, be a cryptosystem that provides authenticated encryption. Consider the following constructions and choose the correct option:

   i. $E_1(k,m) \to (c,c)$, where $E(k,m) \to c$ and $D_1(k,(c_1,c_2)) := D(k,c_1)$.

   ii. $E_2(k,m) \to (c,c)$, where $E(k,m) \to c$ and $D_2(k,(c_1,c_2)) := D(k,c_1)$, if $c_1 = c_2$, else output $\perp$.

   a. Only construction I is CPA secure and provides ciphertext integrity

   b. Only construction II is CPA secure and provides ciphertext integrity

   c. Both constructions I and II only provide CPA security and not ciphertext integrity

   d. Both constructions I and II only provide ciphertext integrity and not CPA security

   e. Both constructions I and II provide CPA security and ciphertext integrity

   The encryption process in both the schemes are the same and is CPA-secure. More specifically, given the challenge ciphertext $(c^\star, c^\star)$, a PPT adversary cannot significantly distinguish apart, whether it is an encryption of m_0 or m_1, or else it implies that given only $c^\star$, the adversary can significantly distinguish apart whether m_0 or m_1 is encrypted in $c^\star$. And, both of the constructions provide ciphertext integrity. This can be proved by contradiction. For the first construction, assume there exists an adversary $\mathcal{A}$ that can produce a ciphertext (c', c') such that it decrypts to some message m' from the message-space. We can construct an adversary $\mathcal{A}'$ using the adversary $\mathcal{A}$ that can produce c' as the ciphertext for the given cryptosystem $(E(k,m), D(k,c))$, which will then decrypt to m', a valid message from the message-space. But, this is a contradiction as the given cryptosystem provides authenticated encryption. Hence, there exists no such adversary $\mathcal{A}'$. Similar argument can be given for the second construction as well. So the correct answer is **e**.