Solutions for Assignment 8

1. Select the correct option(s):

   a) Composition of a CPA-secure scheme together with a SCMA-secure MAC will always ensure an authenticated encrypted scheme

   b) If message m is made up of a sequence of blocks $m_1, \ldots, m_d$ and MAC algorithm outputs a sequence of tags $t_1, \ldots, t_d$ respectively for each of the blocks, then it is easy to forge a MAC on a new message by reordering the tags

   c) Choosing separate keys for encryption and authentication is not needed if the correct order of encryption and authentication is chosen to obtain a secure authenticated encryption scheme

   d) Padding Oracle attack is based on the error response sent by the receiver

   The first statement is incorrect, because as discussed in the lectures, not every composition of a CPA-secure cipher and a secure MAC necessary leads to an authenticated encryption scheme. The second statement is a correct statement. Supposed adversary learns the tag $(t_1, \ldots, t_d)$ for a message $m = (m_1, \ldots, m_d)$. Then it can come up with a tag $(t_2, t_1, t_3, \ldots, t_d)$ for a new message $m' = (m_2, m_1, m_3, \ldots, m_d)$. The third statement is also incorrect, as it has been demonstrated in the lectures that the encrypt-then-authenticate approach is secure, only if the encryption component and MAC component are instantiated with independent keys. The fourth statement is correct. So the answers are **b** and **d**.

2. Which of the following is(are) correct for the key-exchange problem?

   a) The goal of the sender and receiver is to agree upon a random common key, over a public channel

   b) Stronger security notion of key-exchange protocol requires the adversary to unable to distinguish between the output key and a uniformly random element from the key space, except with a negligible probability

   c) The goal of the sender and receiver is to agree upon a fixed common key, over a private channel

   d) Weaker security notion of key-exchange protocol requires the adversary to unable to compute the output key, except with a negligible probability

   The first statement is correct, as the communication between sender and receiver happens over a public channel. And their goal is agree upon a random and private key. So, the third statement is incorrect. The second and fourth statements are true, which follows from the definition of strong security and weak security of key-exchange protocols. So the answers are **a**, **b** and **d**.

3. Let sender and receiver have a pre-shared, random and private AES key k. Then consider the following method of authenticating messages of size which is a multiple of 64 bits: to authenticate a message $m \in \{\{0,1\}^{64}\}^{\leq \ell}$ containing ℓ blocks $m_1, \ldots, m_\ell$ each of size 64 bits, the tag-generation algorithm outputs $t = (t_1, \ldots, t_\ell)$ as the tag, where $t_i = \text{AES}_k(m_i || < \ell >)$. Here $< \ell >$ denotes a 64-bit representation of the integer ℓ, the number of blocks in m. Accordingly, the tag-verification algorithm performs the corresponding verification steps. Identify the correct statement(s) from the following.

   a) The above MAC is randomized and hence is SCMA-secure

   b) The above MAC is deterministic and hence is CMA-secure

   c) The above MAC is neither CMA-secure nor SCMA-secure

   d) The above MAC when used in the encrypt-and-authenticate approach leads to an authenticated encryption scheme

   e) The adversary can always win the MAC forgery game

   The MAC is neither CMA-secure, nor SCMA-secure and hence can never lead to an authenticated encryption scheme. Consider the following mix-and-match attack. The adversary asks for the MAC on messages $m = (m_1, \ldots, m_\ell)$ and $m' = (m'_1, \ldots, m'_\ell)$, where $m_i \neq m'_i$, for $i = 1, \ldots, \ell$. Say the resultant tags are $t = (t_1, \ldots, t_\ell)$ and $t' = (t'_1, \ldots, t'_\ell)$ respectively. Then the tag on the message $m'' = (m_1, m'_2, m_3, m'_4, \ldots, m_{\ell-1}, m'_\ell)$ will be $(t_1, t'_2, t_3, t'_4, \ldots, t_{\ell-1}, t'_\ell)$, which can be easily computed by the adversary and hence adversary can always win the MAC forgery game. So the answers are **c** and **e**.

4. Select the correct option(s):

   a) A cyclic group has one or more generators

   b) Group $(Z_5, +_5)$ has 5 generators

   c) The order of the group $(Z_p^*, \cdot_p)$ where p is prime, is a prime number

   d) $46^{51} \mod 55 = 46$

   The first statement is true, as each cyclic group definitely has one generator, but it could have more than 1 generator. The second statement is false, as $\mathbb{Z}_5 = \{0, \ldots, 4\}$, and all the elements except the identity element, namely 0, is a generator, so it has total 4 generators. The third statement is false, as the size of $\mathbb{Z}_p^\star$ is $p-1$. In the fourth statement, the modulo $N = 55 = 5 \times 11$ and so $p = 5$ and $q = 11$, which are the prime factors of 55. Now $\phi(55) = |\mathbb{Z}_{55}^\star| = (5-1)\cdot(11-1) = 40$. Also $GCD(46, 55) = 1$ and hence $46 \in \mathbb{Z}_{55}^\star$. This further implies that the order of the element 46 is 40, implying that $46^{40} \mod 55 = 1$, where 1 is the identity element of the group $(\mathbb{Z}_{55}^\star, \cdot \mod 55)$. Now $46^{51} \mod 55 = (46^{40} \mod 55) \cdot (46^{11} \mod 55) = 46^{11} \mod 55$. We can write $46^{11} \mod 55$ as $(46^3 \mod 55)\cdot(46^3 \mod 55)\cdot(46^3 \mod 55)\cdot(46^2 \mod 55)$. Now $(46^3 \mod 55) = 41$ and so $(46^2 \mod 55) = 26$. So the overall answer is $(41 \cdot 41 \cdot 41 \cdot 26) \mod 55 = 46$. So the answers are **a** and **d**.

5. Consider a secure PRF $F_k : \{0,1\}^n \rightarrow \{0,1\}^n$, using which we construct a keyed function $F'_k : \{0,1\}^{2n} \rightarrow \{0,1\}^{2n}$, where $F'_k(x_1||x_2) \stackrel{def}{=} F_k(x_1)||F_k(F_k(x_2))$ and $x = x_1||x_2$, where $x_1, x_2 \in \{0,1\}^n$.

   a. Function F' is a secure PRF and when used directly leads to a CMA-secure MAC

   b. Function F' is not a secure PRF

   c. Function F' is a secure PRF but when used directly does not lead to a CMA-secure MAC

   d. Function F' when used directly does not lead to a CMA-secure MAC

   The construction F'_k is not a a secure PRF (and hence it does not lead to a secure MAC). An adversary upon learning the output of $F'_k(x_1||x_2)$ and $F'_k(x'_1||x'_2)$ can always and easily compute the output of $F'_k(x_1||x'_2)$, which it can do for a TRF only with a negligible probability. So the answers are **b** and **d**.