Solutions for Assignment 9

1. Select the incorrect option(s):

   a. If p is a prime then $\mathbb{Z}_p^\star$ is a cyclic group of order p.

   b. The point at infinity $\mathcal{O}$ acts as the identity element for the group $(E, +)$ where E is the set of points on a non-singular elliptic curve.

   c. The negative of a point on an elliptic curve is its reflection in the y-axis.

   d. In a prime-order group every element of the group is a generator.

   The first statement is false, as $\mathbb{Z}_p^\star$ is a cyclic group of order $p - 1$.

   The second statement is true.

   The third statement is false, as the negative of a point on an elliptic curve is its reflection in the x-axis.

   The last statement is false, as the identity element is never a generator for a cyclic group.

   So the answer is **a, c** and **d**.

2. Which of the following point(s) satisfy the curve $y^2 \equiv x^3 + 22x + 25 \mod 47$:

   a. $(25, 28)$.

   b. $(23, 33)$.

   c. $(3, 46)$.

   d. $(5, 7)$.

   For $(25, 28)$, we have $LHS = 784 \mod 47 = 32$ and $RHS = 16200 \mod 47 = 32$. Since $LHS = RHS$, the point lies on the curve.

   For $(25, 33)$, we have $LHS = 1089 \mod 47 = 8$ and $RHS = 12698 \mod 47 = 8$. Since $LHS = RHS$, the point lies on the curve.

   For $(3, 46)$, we have $LHS = 2116 \mod 47 = 1$ and $RHS = 118 \mod 47 = 24$. Since $LHS \neq RHS$, the point does not lie on the curve.

   For $(5, 7)$, we have $LHS = 49 \mod 47 = 2$ and $RHS = 260 \mod 47 = 25$. Since $LHS \neq RHS$, the point does not lie on the curve.

   So the answer is **a** and **b**.

3. Choose the correct option(s) with respect to public key setting:

   a. The ciphertext may not be always correctly decrypted to its corresponding plaintext.

   b. An adversary does not have access to encryption oracle in a COA setting.

   c. Single-message CPA secure also implies multi-message CPA secure only if the encryption algorithm is randomized.

   d. Perfect secrecy is easy to achieve.

   The first statement is correct, because if the key-generation algorithm outputs "incorrect" keys, then there will be an error in the correctness property.

   For instance, if we take the RSA cryptosystem, then if one uses randomized algorithms to check if generated p and q are primes or not, then there is a small probability that one ends up picking composite p and q and hence the corresponding $N = pq$ and (e, d) will not satisfy the properties of RSA public and secret keys.

   The second statement is incorrect, as the adversary has access to encryption oracle in a COA setting.

   The third statement is correct, because if the encryption process is deterministic, then it is not even single-message COA-secure (hence not single-message CPA-secure).

And the last statement is incorrect, because if the adversary is computationally unbounded, then from the value of the public key, it can always find out the corresponding secret key, by doing brute force over the key space.

So the answer is **a** and **c**.

4. Which of the following statement(s) is/are correct?

   a. DLog is easy to solve for some additive cyclic groups.

   b. DLog is easy to solve for some multiplicative cyclic groups.

   c. CDH assumption is stronger than the DDH assumption.

   d. Efficiently solving DDH problem implies efficiently solving DLog problem.

   e. Efficiently solving CDH problem implies efficiently solving DDH problem.

   The first two statements are correct, as the DLog problem need not be computationally difficult to solve in every group. For instance, one can efficiently solve the DLog problem in the additive cyclic group $(\mathbb{Z}_p, + \mod p)$, where p is a prime.

   The third statement is incorrect.

   The fourth statement is incorrect because the DDH assumption is considered a stronger assumption compared to the DLog assumption.

   The last statement is correct.

   So the answer is **a, b** and **e**.

5. Let $\mathbb{G}$ be a prime order cyclic group of order q with a generator g. Then a commitment scheme is defined as follows: $\alpha \in \mathbb{Z}_q$ is the value the sender wants to commit to the receiver. To do so, it picks a random r from $\mathbb{Z}_q$ and sends the commitment $(r, g^{\alpha r})$ to the receiver. To open the committed value, the sender reveals α and the receiver does the verification accordingly. Which of the following statement(s) is/are true for this commitment scheme?

   a. The scheme does not satisfy binding, even if DLog assumption is true for $\mathbb{G}$.

   b. The scheme does not satisfy hiding, even if DLog assumption is true for $\mathbb{G}$.

   c. The scheme does not satisfy binding, even if DDH assumption is true for $\mathbb{G}$.

   d. The scheme does not satisfy hiding, even if DDH assumption is true for $\mathbb{G}$.

   e. None of the above.

   The scheme does not satisfy the hiding property: let the adversary submits (m_0, m_1) in the hiding experiment and receives the challenge commitment $(r, g^{m_b r})$. The adversary can then recompute the commitments of m_0 and m_1 with respect to r and by comparing it with $g^{m_b r}$, it can find out whether it got the commitment of m_0 or m_1.

   The scheme also does not satisfy the binding property: Let $\alpha \neq \alpha'$ be two values. A corrupt sender can pick $r = 0$ and send the commitment $(0, g^{\alpha r}) = (0, e)$ during the commit phase, where $e = g^0$ is the identity element. Later, it can reveal $\alpha' \neq \alpha$. It is easy to see that the verification will be successful, even with α'; namely, the receiver will recompute the commitment $g^{\alpha' r}$ and will find that it is the same as e, the value received during the commit phase.

   So the answer is **a, b, c** and **d**.