Problems

10.1 Users A and B use the Diffie-Hellman key exchange technique with a common prime \( q = 71 \) and a primitive root \( \alpha = 7 \).
   a. If user A has private key \( X_A = 5 \), what is A's public key \( Y_A \)?
   b. If user B has private key \( X_B = 12 \), what is B's public key \( Y_B \)?
   c. What is the shared secret key?

10.2 Consider a Diffie-Hellman scheme with a common prime \( q = 11 \) and a primitive root \( \alpha = 2 \).
   a. Show that 2 is a primitive root of 11.
   b. If user A has public key \( Y_A = 9 \), what is A's private key \( X_A \)?
   c. If user B has public key \( Y_B = 3 \), what is the shared secret key \( K \), shared with A?

10.3 In the Diffie-Hellman protocol, each participant selects a secret number \( x \) and sends the other participant \( \alpha^x \mod q \) for some public number \( \alpha \). What would happen if the participants sent each other \( x^\alpha \) for some public number \( \alpha \) instead? Give at least one
method Alice and Bob could use to agree on a key. Can Eve break your system without finding the secret numbers? Can Eve find the secret numbers?

10.4 This problem illustrates the point that the Diffie-Hellman protocol is not secure without the step where you take the modulus; i.e. the "Indiscrete Log Problem" is not a hard problem! You are Eve, and have captured Alice and Bob and imprisoned them. You overhear the following dialog.

**Bob:** Oh, let's not bother with the prime in the Diffie-Hellman protocol, it will make things easier.

**Alice:** Okay, but we still need a base \( a \) to raise things to. How about \( g = 3 \)?

**Bob:** All right, then my result is 27.

**Alice:** And mine is 243.

What is Bob's secret \( X_B \) and Alice's secret \( X_A \)? What is their secret combined key? (Don't forget to show your work.)

10.5 Section 10.2 describes a man-in-the-middle attack on the Diffie-Hellman key exchange protocol in which the adversary generates two public-private key pairs for the attack. Could the same attack be accomplished with one pair? Explain.

10.6 In 1985, T. ElGamal announced a public-key scheme based on discrete logarithms, closely related to the Diffie-Hellman technique. As with Diffie-Hellman, the global elements of the ElGamal scheme are a prime number \( q \) and \( a \), a primitive root of \( q \). A user A selects a private key \( X_A \) and calculates a public key \( Y_A \) as in Diffie-Hellman. User A encrypts a plaintext \( M < q \) intended for user B as follows:

1. Choose a random integer \( k \) such that \( 1 \leq k \leq q - 1 \).
2. Compute \( K = (Y_B)^k \mod q \).
3. Encrypt \( M \) as the pair of integers \((C_1, C_2)\) where
   \[
   C_1 = a^k \mod q \quad C_2 = KM \mod q
   \]

User B recovers the plaintext as follows:

1. Compute \( K = (C_1)^{x_A} \mod q \).
2. Compute \( M = (C_2K^{-1}) \mod q \).

Show that the system works; that is, show that the decryption process does recover the plaintext.

10.7 Consider an ElGamal scheme with a common prime \( q = 71 \) and a primitive root \( a = 7 \).

a. If B has public key \( Y_B = 3 \) and A chose the random integer \( k = 2 \), what is the ciphertext of \( M = 30 \)?

b. If A now chooses a different value of \( k \), so that the encoding of \( M = 30 \) is \( C = (59, C_2) \), what is the integer \( C_2 \)?

10.8 Rule (5) for doing arithmetic in elliptic curves over real numbers states that to double a point \( Q \), draw the tangent line and find the other point of intersection \( S \). Then \( Q + Q = 2Q = -S \). If the tangent line is not vertical, there will be exactly one point of intersection. However, suppose the tangent line is vertical? In that case, what is the value \( 2Q \)? What is the value \( 3Q \)?

10.9 Demonstrate that the two elliptic curves of Figure 10.9 each satisfy the conditions for a group over the real numbers.

10.10 Is \((4,7)\) a point on the elliptic curve \( y^2 = x^3 - 5x + 5 \) over real numbers?

10.11 On the elliptic curve over the real numbers \( y^2 = x^3 - 36x \), let \( P = (-3.5, 9.5) \) and \( Q = (-2.5, 8.5) \). Find \( P + Q \) and \( 2P \).

10.12 Does the elliptic curve equation \( y^2 = x^3 + 10x + 5 \) define a group over \( \mathbb{Z}_7 \)?

10.13 Consider the elliptic curve \( E_{11}(1, 6) \); that is, the curve is defined by \( y^2 = x^3 + x + 6 \) with a modulus of \( p = 11 \). Determine all of the points in \( E_{11}(1, 6) \). \textit{Hint:} Start by calculating the right-hand side of the equation for all values of \( x \).

10.14 What are the negatives of the following elliptic curve points over \( \mathbb{Z}_5 \)? \( P = (5, 8); Q = (3, 0); R = (0, 6). \)

10.15 For \( E_{11}(1, 6) \), consider the point \( G = (2, 7) \). Compute the multiples of \( G \) from \( 2G \) through \( 13G \).
10.16 This problem performs elliptic curve encryption/decryption using the scheme outlined in Section 10.4. The cryptosystem parameters are $E_{11}(1,6)$ and $G = (2, 7)$. B’s secret key is $n_B = 7$.

a. Find B’s public key $P_B$.

b. A wishes to encrypt the message $P_w = (10, 9)$ and chooses the random value $k = 3$. Determine the ciphertext $C_w$.

c. Show the calculation by which B recovers $P_w$ from $C_w$.

10.17 The following is a first attempt at an Elliptic Curve signature scheme. We have a global elliptic curve, prime $p$, and “generator” $G$. Alice picks a private signing key $X_A$ and forms the public verifying key $Y_A = X_A G$. To sign a message $M$:

- Alice picks a value $k$.
- Alice sends Bob $M, k$ and the signature $S = M - kX_A G$.
- Bob verifies that $M = S + kY_A$.

a. Show that this scheme works. That is, show that the verification process produces an equality if the signature is valid.

b. Show that the scheme is unacceptable by describing a simple technique for forging a user’s signature on an arbitrary message.

10.18 Here is an improved version of the scheme given in the previous problem. As before, we have a global elliptic curve, prime $p$, and “generator” $G$. Alice picks a private signing key $X_A$ and forms the public verifying key $Y_A = X_A G$. To sign a message $M$:

- Bob picks a value $k$.
- Bob sends Alice $C_1 = kG$.
- Alice sends Bob $M$ and the signature $S = M - X_A C_1$.
- Bob verifies that $M = S + kY_A$.

a. Show that this scheme works. That is, show that the verification process produces an equality if the signature is valid.

b. Show that forging a message in this scheme is as hard as breaking (ElGamal) Elliptic Curve Cryptography. (Or find an easier way to forge a message?)

c. This scheme has an extra “pass” compared to other cryptosystems and signature schemes we have looked at. What are some drawbacks to this?