Problem 8.1.

1. Which of the following are commutative groups? For the commutative groups, give the identity element and the inverse of any element.
   (a) $(\mathbb{Z}, \cdot)$
   (b) $(\mathbb{R}^n, +)$, for some fixed positive integer n, where $+$ is the componentwise addition
   (c) $(\mathbb{R}^n, \cdot)$, where $\cdot$ is the scalar product: $(u_1, \ldots, u_n) \cdot (v_1, \ldots, v_n) = \sum_{i=1}^{n} u_i v_i$
   (d) $(\{z \in \mathbb{C} | z^n = 1\}, \cdot)$, for some fixed positive integer n
   (e) $(e^{i\theta}, \cdot)$, where $\theta \in \mathbb{R}$ and i is the unit complex number such that $i^2 = -1$
   (f) $(\{0, 1\}, \wedge)$, where $\wedge$ is the logical "and" operation
   (g) $(\mathbb{Z}/5\mathbb{Z}, \cdot)$
   (h) $(\mathbb{Z}/5\mathbb{Z} \setminus \{[0]_5\}, \cdot)$
   (i) $(\mathbb{Z}/5\mathbb{Z} \setminus \{[0]_5\}, +)$
2. Are the following commutative groups isomorphic? If not - prove it. If yes - give the tables and the isomorphism:
   (a) $G_1 = (\mathbb{Z}/5\mathbb{Z}^*, \cdot)$ and $H_1 = (\{z \in \mathbb{C} | z^4 = 1\}, \cdot)$
   (b) $G_2 = (\mathbb{Z}/6\mathbb{Z}^*, \cdot)$ and $H_2 = (\mathbb{Z}/3\mathbb{Z}^*, \cdot)$
   (c) $G_3 = (\mathbb{Z}/2\mathbb{Z}, +) \times (\mathbb{Z}/2\mathbb{Z}, +)$ and $H_3 = (\mathbb{Z}/4\mathbb{Z}, +)$
   (Hint: Check the orders of the elements.)
   (d) $G_4 = (\mathbb{Z}/15\mathbb{Z}^*, \cdot)$ and $H_4 = (\mathbb{Z}/7\mathbb{Z}, +)$

Problem 8.2.

1. Compute the order of each element in the commutative group $(\mathbb{Z}/18\mathbb{Z}^*, \cdot)$.
2. Can you find an integer k such that $(\mathbb{Z}/18\mathbb{Z}^*, \cdot)$ and $(\mathbb{Z}/k\mathbb{Z}, +)$ are isomorphic? If yes, give an example of such isomorphism.

Problem 8.3.

1. Show that (x, y) is invertible in $(\mathbb{Z}/17\mathbb{Z}, \cdot) \times (\mathbb{Z}/121\mathbb{Z}, \cdot)$ if and only if x is invertible in $(\mathbb{Z}/17\mathbb{Z}, \cdot)$ and y is invertible in $(\mathbb{Z}/121\mathbb{Z}, \cdot)$.
2. How many invertible elements are in $(\mathbb{Z}/17\mathbb{Z}, \cdot) \times (\mathbb{Z}/121\mathbb{Z}, \cdot)$?
3. Solve the following equation where the unknown is $n \in \mathbb{N}$:
   $$2^n \equiv 1 \mod 13$$
4. Solve the equation $x^{19} = x$ for $x \in (\mathbb{Z}/19\mathbb{Z}, \cdot)$.

Problem 8.4.

Consider the El Gamal cryptosystem.

1. Select $p = 47$. Verify that $g = 5$ is indeed a generator of $(\mathbb{Z}/47\mathbb{Z}^*, \cdot)$.
2. Alice wants to send the plaintext $t = 13$ using $g = 5$ to Bob. Alice receives from Bob $g^x \bmod 47 = 31$ (with x being Bob's secret). Alice's secret number is $y = 2$. What two integers will Alice send to Bob to share the plaintext t?
3. You now learn Bob's secret, $x = 3$ (indeed $g^3 \bmod 47 = 31$). Show how Bob can get back the plaintext from the two integers Alice sent him.
4. Select $p = 61$. Is $g = 9$ a good choice? Eve observes the communication between Alice and Bob:
   - Bob sends $g^x = 58$ to Alice.
   - Alice replies with $(g^y, g^{xy} \cdot t) = (34, 28)$.

   Can Eve recover the message t shared between Alice and Bob? *(Hint: Determine the order of g modulo 61.*

Problem 8.5.

1. Let $(G, \star)$ be a finite commutative group. Consider the following encryption method. The message that Alice wants to send to Bob is an element $t \in G$. The key is a uniformly distributed random element $k \in G$, selected independently of the message t. Alice sends the ciphertext $c = k \star t$ to Bob. Does it provide perfect secrecy?
2. Let $m > 1$ be an integer, consider a message $t \in \{0, 1, \ldots, m-1\}$ and a uniformly distributed key $k \in \{0, 1, \ldots, m-1\}$. Which of the following encryption methods provide perfect secrecy?
   (a) $c = t + k$
   (b) $c = t + k \bmod m$
3. Let $m > 1$ be an integer, consider a message $t \in \{1, \ldots, m-1\}$ and a uniformly distributed key $k \in \{1, \ldots, m-1\}$. Which of the following encryption methods provide perfect secrecy?
   (a) $c = t \cdot k$
   (b) $c = t \cdot k \bmod m$