Exercise 8-1  Recall the definition of the group \( \mathbb{Z}_N^* \) and that its order, i.e. the number of elements, is denoted \( \phi(N) \).

a) Show \( \phi(p^e) = p^{e-1}(p - 1) \) for any prime \( p \) and any \( e \leq 1 \).

Solution (Sketch): The group \( \mathbb{Z}_{p^e}^* \) consists of all numbers in \{1, \ldots, p^e - 1\} that are relatively prime to \( p^e \). A number is relatively prime to \( p^e \) if and only if it is not divisible by \( p \). This means that \( \mathbb{Z}_{p^e} = \{1, \ldots, p^e - 1\} \setminus \{k \cdot p \mid 1 \leq k \leq p^{e-1} - 1\} \). The two sets have \( p^e - 1 \) and \( p^{e-1} - 1 \) elements respectively. Hence, \( \phi(p^e) = (p^e - 1) - (p^{e-1} - 1) = p^{e-1}(p - 1) \).

b) Show that \( \phi(pq) = \phi(p)\phi(q) \) if \( p \) and \( q \) are relatively prime.

Hint: Use the Chinese Remainder Theorem.

Solution (Sketch): The Chinese Remainder Theorem can be expressed so that the function \( f(x) = (x \mod p, x \mod q) \) is a group isomorphism \( \mathbb{Z}_{pq}^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^* \). The bijection immediately gives the required \( \phi(pq) = \phi(p)\phi(q) \).

Exercise 8-2  Let \( p \) and \( q \) be the primes 17 and 23. Let \( N := pq \) and \( e := 3 \).

a) Compute a number \( d \), such that \( d = e^{-1} \mod \phi(N) \).

Solution (Sketch): The extended Euclidean Algorithm computes, for any given \( x \) and \( y \), two numbers \( a \) and \( b \), such that \( a \cdot x + b \cdot y = \gcd(x, y) \). In this case, we have \( 1 = \gcd(e, \phi(N)) \), so we can compute \( a \) and \( b \) with \( a \cdot e + b \cdot \phi(N) = 1 \) using the extended Euclidean Algorithm.

But \( a \cdot e + b \cdot \phi(N) = a \cdot e \mod \phi(N) \), so taking \( d := a \mod N \) gives the sought-after number.

Concretely, \( \phi(N) = 16 \cdot 22 = 352 \). The extended GCD algorithm gives \(-117 \cdot 3 + 352 = 1\), so \( d = 235 \) is a solution.
b) Encrypt the message abc using Plain RSA, where $Enc(m) = m^e \mod N$ and $Dec(m) = m^d \mod N$. Use an appropriate encoding. Verify that it decrypts correctly.

**Solution (Sketch):** By Exercise 8-1, we know that $\mathbb{Z}_{pq}^*$ has $16 \cdot 22 = 352$ elements, namely:

\begin{align*}
&\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 18, 19, 20, 21, 22, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 35, 36, 37, 38, 39, 40, \\
& 41, 42, 43, 44, 45, 47, 48, 49, 50, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, \\
& 114, 116, 117, 118, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 137, 139, 140, 141, 142, 143, 144, \\
& 175, 176, 177, 178, 179, 180, 181, 182, 183, 185, 186, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, \\
& 295, 296, 297, 298, 300, 301, 302, 303, 304, 305, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 324, 325, \\
& 385, 386, 387, 388, 389, 390\}
\end{align*}

To encode the message, we can use an ASCII encoding, for example. Encoded in ASCII, abc becomes 97, 98, 99. To represent abc as elements of $\mathbb{Z}_{pq}^*$, we can therefore use the 97-th, 98-th and 99-th elements of $\mathbb{Z}_{pq}^*$. These are 108, 109 and 110.

The encryptions of these are

\begin{align*}
301 &= 108^3 \mod N \\
37 &= 109^3 \mod N \\
36 &= 110^3 \mod N
\end{align*}

One verifies the correct decryption:

\begin{align*}
108 &= 301^{235} \mod N \\
109 &= 37^{235} \mod N \\
110 &= 36^{235} \mod N
\end{align*}

Note, however, Plain RSA is not CPA-secure (randomisation is needed in the encryption), and that this way of encoding messages corresponds to ECB mode, which is also insecure. Recall the chapter on the modes of operation of block ciphers.

**Exercise 8-3**

a) Find all the elements of the group $\mathbb{Z}^*_{13}$ of that generate cyclic subgroups of prime order.
A description of a finite cyclic group $G$. In practice, one often uses subgroups of prime order of $\mathbb{Z}$.

The Diffie-Hellman protocol uses a group generating algorithm that outputs a triple $(p, q, g)$ as the output of the group generating algorithm. This denotes the subgroup of $\mathbb{Z}_p^*$ of order $q$ that is generated by $g \in \mathbb{Z}_p^*$, i.e., $G = \{g^i \mod p \mid i \in \mathbb{N}\}$.

**Solution (Sketch):** $\mathbb{Z}_{13}^* = \{1, 2, \ldots, 12\}$ The cyclic subgroup generated by an element $g$ of this group is $\{g^k \mid k \geq 0\}$.

In this case:

- 1 generates $\{1\}$.
- 2 generates $\{1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7\}$.
- 3 generates $\{1, 3, 9\}$.
- 4 generates $\{1, 4, 3, 12, 9, 10\}$.
- 5 generates $\{1, 5, 12, 8\}$.
- 6 generates $\{1, 6, 10, 8, 9, 2, 12, 7, 3, 5, 4, 11\}$.
- 7 generates $\{1, 7, 10, 5, 9, 11, 12, 6, 3, 8, 4, 2\}$.
- 8 generates $\{1, 8, 12, 5\}$.
- 9 generates $\{1, 9, 3\}$.
- 10 generates $\{1, 10, 9, 12, 3, 4\}$.
- 11 generates $\{1, 11, 4, 5, 3, 7, 12, 2, 9, 8, 10, 6\}$.
- 12 generates $\{1, 12\}$.

Note also that the order of each subgroup divides the order of the whole group, which is always true (Lagrange theorem).

This means that the elements 3, 9 and 12 generate subgroups of prime order.

**Exercise 8-4** The Diffie-Hellman protocol uses a group generating algorithm that outputs a description of a finite cyclic group $G$ together with its order $q$ and a generating element $g$.

In practice, one often uses subgroups of prime order of $\mathbb{Z}_p^*$, for some $p$. Then, one can take the triple $(p, q, g)$ as the output of the group generating algorithm. This denotes the subgroup of $\mathbb{Z}_p^*$ of order $q$ that is generated by $g \in \mathbb{Z}_p^*$, i.e., $G = \{g^i \mod p \mid i \in \mathbb{N}\}$.

b) Show: If $g$ generates $\mathbb{Z}_p^*$, where $p > 2$ is prime, then $g^2$ generates $\{x \in \mathbb{Z}_p^* \mid \exists y \in \mathbb{Z}_p^*, x \equiv y^2 \mod p\}$.

**Solution (Sketch):** First, the subgroup generated by $g^2$ must be a subset of $\{x \in \mathbb{Z}_p^* \mid \exists y \in \mathbb{Z}_p^*, x \equiv y^2 \mod p\}$. For any $x = (g^2)^k$, we can take $y$ to be $g^k$ and have the required $x \equiv y^2 \mod p$.

For the reverse inclusion, it remains to show: $x = y^2 \mod p$ implies $x = (g^2)^k \mod p$ for some $k$. Since $g$ is a generator of the whole group, we have $x = g^m \mod p$ and $y = g^n \mod p$ for some $m$ and $n$.

From $x = y^2 \mod p$ we get $g^m = g^{2n}$. This implies $m = 2n \mod \phi(p)$. (It is a general fact that $g^a = g^b$ in a cyclic group $G$ implies $a = b \mod \text{order}(G)$). Since $p-1$ is a prime, we know that $\phi(p) = p - 1$ is an even number. But then $m = 2n \mod p - 1$ implies that $m$ is even. This shows that $x = (g^2)^{m/2}$, i.e., that $x$ is in the subgroup generated by $g^2$. 
Suppose in the first step of the Diffie-Hellman protocol, the group generating algorithm output 
$(11, 5, 3)$. Work through the rest of one run of the algorithm with this group.

**Solution (Sketch):**

- Alice runs $G(n)$. Suppose the result is $(11, 5, 3)$. Alice sends this to Bob.
- Alice chooses random $x$ in $\{1, \ldots, q - 1\}$, say 2 and computes $3^x = 9$
- Bob chooses random $y$ in $\{1, \ldots, q - 1\}$, say 3 and computes $3^y = 5$
- Alice outputs the key $5^x = 3$.
- Bob outputs the key $9^y = 3$. 