Problem 1. Recall that the implementation of the RSA cryptosystem heavily relies on modular arithmetic, Euler’s totient (phi) function, and Euler’s Theorem.

The process of generating the public-private key pair is as follows:

1. First, the receiver chooses two (large) prime numbers $p$ and $q$. The product $n = pq$ is half of the public key.

2. The receiver calculates $\varphi(n) = (p-1)(q-1)$ and chooses an integer $e$ that is relatively prime to $\varphi(n)$. This integer is the other half of the public key, and with that being said, the public key is usually represented as the pair $(n, e)$.

3. The receiver calculates the modular inverse $d$ of $e$ modulo $\varphi(n)$. In other words, the receiver solves the following linear congruence $de \equiv 1 \pmod{\varphi(n)}$. The calculation can be done efficiently using Extended Euclidean Algorithm and the integer $d$ is the private key (or the pair $(n, d)$ as illustrated in the textbook).

4. The receiver distributes the public key $(n, e)$ to the sender and keeps $(n, d)$ to themselves.

The process of transmitting some message $m$ is as follows:

1. The sender converts their message $m$ into a number (using ASCII or Unicode table).

2. The sender, upon receiving the public key $(n, e)$ from the receiver, calculates $c \equiv m^e \pmod{n}$ where $c$ is the encrypted message (or sometimes called cyphertext). This is the only information (along with the public key) that the attacker can have.

3. The receiver computes $c^d \equiv m \pmod{n}$ thus retrieving the original integer value $m$ of the message and convert it into the corresponding character.

Why this works: the most basic goal is to be able to “decrypt” the encrypted message, in other words, for $m \in \mathbb{Z}_n$, we want $c^d = (m^e)^d = m$. The main idea for the proof is to use Euler’s Theorem. Broadly speaking, if $m \in \mathbb{Z}_n^*$, then it trivially follows from Euler’s Theorem that $m^{ed} \equiv m \pmod{n}$. Now assume we have an arbitrary $m \in \mathbb{Z}_n$. We first use Euler’s Theorem to prove that $m^{ed} \equiv m \pmod{p}$. Then, apply the same idea to show that $m^{ed} \equiv m \pmod{q}$ which, taken together with the previous congruence, implies $m^{ed} \equiv m \pmod{pq}$ and the proof is complete (see page 100 in the textbook for the full proof).
**Demo:** Generate the public and private key with primes $p = 11$ and $q = 17$ and the assumption that the receiver chooses an integer $e = 3$ which is relatively prime to $n = pq = 187$. Then, simulate the process of transmitting a message whose integer value $m = 87$. 
Problem 2. Find the multiplicative inverse of 11 modulo 26. (Hint: apply Extended Euclidean Algorithm on inputs $a = 26$ and $b = 11$)