0. This problem is a reading exercise, and will not be graded. Read the proof of Theorem 1 in Jonathan Katz’s Lecture 31.

1. Suppose we are using El-Gamal encryption for messages from some known cyclic group $G$; recall that to encrypt a message $m \in G$, we choose a random $r \in \{0, 1, \ldots, |G| - 1\}$ and send $(g^r, h^r m)$ as ciphertext. (Also, $g$ is a randomly chosen generator for $G$, and is publicly known.) Now suppose the adversary has been able to see two ciphertexts for the same plaintext $M$, and that these two ciphertexts are of the form $(u, v)$ and $(u^2, w)$ for some elements $u, v, w$ of $G$. Show how the adversary can infer the plaintext $M$ from this information.

2. Consider Theorem 1 in Jonathan Katz’s Lecture 32, on two different notions of security for public-key cryptosystems. Katz’s Lecture 32, as well as our discussion in class, only prove the theorem for the case $\ell = 2$. Prove the theorem for an arbitrary value of $\ell$.

3. (For graduate students, and extra credit for undergraduate students.) Suppose $n$ is composite and is not a Carmichael number; i.e., there exists some $m \in \mathbb{Z}_n^*$ such that $m^{n-1} \not\equiv 1 \mod n$. Then, show that the simple primality test for $n$ shown in class succeeds with probability at least $1/2$. In more detail, suppose we choose an $a$ at random from the set $\{1, 2, \ldots, n-1\}$. We output “composite” if at least one of the following two conditions hold: (i) $\gcd(a, n) \neq 1$, or (ii) $a^{n-1} \not\equiv 1 \mod n$. Show that we will output “composite” with probability at least $1/2$.

Hint: Suppose $G$ is a group. Then, a subset $S$ of the elements of $G$ is a subgroup of $G$ if and only if the following two conditions hold: (i) $\forall a \in S, a^{-1} \in S$, and (ii) $\forall a, b \in S, ab \in S$. (The values $a^{-1}$ and $ab$ here are computed in the group $G$ as usual.) Then, Lagrange’s Theorem says that if $G$ is a finite group and $S$ is a subgroup of $G$, then the cardinality of $G$ is divisible by the cardinality of $S$. Now, in the given problem, apply Lagrange’s Theorem to the group $G = \mathbb{Z}_n^*$ and to a suitably chosen subgroup $S$. 