Sample Quiz 2

Important Notes:

- Quiz date: 16th April (Wed), in class.
- Quiz duration: 50 minutes.
- Chapters covered: Boneh&Shoup Chapters 9-12, examinable learning points can be found in the Github repo.
- Cheat sheets: You are allowed to have **three double-sided A4-size notes**.

Question 1 (Authenticated Encryption): Let (E, D) be an AE-secure cipher. Consider the following derived cipher (E', D'):

- $E'(k, m) := (E(k, m), E(k, m))$,
- $D'(k, (c_0, c_1)) := \begin{cases} D(k, c_0) & \text{if } D(k, c_0) = D(k, c_1), \\ \text{reject} & \text{otherwise.} \end{cases}$

Show that (E', D') is not AE secure.

Question 2 (Public Key Tools)): Let $pk = (n, e)$ and $sk = (n, d)$ be an RSA key pair where n is a product of two primes p and q. What is the relation between e and d? Prove that for any $m \in [1, \ldots, n-1]$, $(m^e)^d = m \pmod{n}$.

Question 3 (Public Key Encryption): Show that the vanilla encryption scheme based on RSA (where $E((n, e), m) = m^e \pmod{n}$) is not CPA secure.

Question 4 (Chosen Ciphertext Secure Public Key Encryption): Let $\mathcal{E} = (G, E, D)$ be a CCA-secure public-key encryption scheme defined over $(\mathcal{M}, \mathcal{C})$ where $\mathcal{C} := \{0,1\}^l$. Consider a modified encryption scheme $\mathcal{E}' = (G, E', D')$ defined over $(\mathcal{M}, \mathcal{C}')$ where $\mathcal{C}' := \{0,1\}^{l+1}$ where

- $E'(pk, m) := E(pk, m) \,\|\, 0$,
- $D'(sk, c) := D(sk, c[:-1])$.

Show that $\mathcal{E}'$ is not CCA secure.