

# Sample Quiz 1

## Important Notes:

- Quiz date: 26th February (Wed), in class.
- Quiz duration: 50 minutes.
- Chapters covered: Boneh&Shoup Chapters 1-7, 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 (Encryption):** Let  $\mathcal{E} = (E, D)$  be a semantically secure cipher. Which one of the following encryption algorithms yields a semantically secure scheme? Either give an attack or provide a security proof via an explicit reduction.

- (a)  $E_1(k, m) = 0 \parallel E(k, m)$ .
- (b)  $E_1(k, m) = m_0 \parallel E(k, m)$  where  $m_0$  is the first bit of  $m$ .

**Question 2 (Stream Cipher):** Let  $G_0$  and  $G_1$  be two PRGs. Define  $G(s_0, s_1) = G_0(s_0) \parallel G_1(s_1)$ . Show that  $G$  is not a secure PRG if either  $G_0$  or  $G_1$  is not a secure PRG.

**Question 3 (Block Cipher):** Let  $F_0$  and  $F_1$  be PRFs with the same input and output spaces. Define

$$F((k_0, k_1), m) = F_0(k_0, m) \oplus F_1(k_1, m).$$

Show that  $F$  is a secure PRF if either  $F_0$  or  $F_1$  is a secure PRF.

**Question 4 (CPA):** Let  $E : \mathcal{K} \times \mathcal{M} \times \mathcal{N} \rightarrow \mathcal{C}$  be an ill-formed implementation of nonce-based AES-CBC as follows.

- Given key  $k$  and an initial nonce  $n$  that is properly generated, the first message  $m_0$  is encrypted as  $c_0 = E(k, m_0, n)$ . ( $n$  is not a part of  $c_0$ .) Let  $\hat{c}_0$  be the last block of  $c_0$ .
- For subsequent messages, a message  $m_i$  is encrypted as  $c_i = E(k, m_i, \hat{c}_{i-1})$ , where  $\hat{c}_{i-1}$  is the last block of ciphertext  $c_{i-1}$ .

Show that the computational cipher based on the encryption scheme described above is not semantically secure against chosen plaintext attack.

*Hint: You can pick the messages adaptively in the security game.*

**Question 5 (MAC):** Let  $H : \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{T}$  be the raw CBC-MAC (without a nonce and no PRF evaluation after CBC). Show that  $H'(k, m) = H(k, m \parallel \langle |m| \rangle)$  where  $\langle |m| \rangle$  is a binary representation of the length of  $m$ . Show that  $H'$  is not a secure PRF (and hence, not a secure MAC).

**Question 6 (Message integrity from universal hashing):** Recall that  $\text{PRF}(\text{UHF})$  composition works by combining a universal hash function  $H$  and a PRF  $F$  as  $F'((k_0, k_1), m) = F(k_1, H(k_0, m))$ . Show that the composition is not secure (as a PRF) if the same key is used for  $H$  and  $F$ . That is,  $F'(k, m) = F(k, H(k, m))$  instead. It suffices to give particular  $H$  and  $F$ , and show a concrete attack with them.