Assignment 7 - 2019.11.13

Submission deadline: 2019.11.20

1. Let (E, D) be a CPA-secure cipher defined over (K, M, C) and let $H_1: M \to T$ and $H_2: C \to T$ be collision resistant hash functions. Define the following two ciphers:

$$E_1(k,m) := \big(E(k,m),\ H_1(m)\big); \quad D_1\big(k,\ (c_1,c_2)\big) := \begin{cases} D(k,c_1) & \text{if } H_1(D(k,c_1)) = c_2 \\ \text{reject} & \text{otherwise} \end{cases}$$

$$E_2(k,m) := \big(E(k,m),\ H_2(c)\big); \quad D_2\big(k,\ (c_1,c_2)\big) := \begin{cases} D(k,c_1) & \text{if } H_2(c_1) = c_2 \\ \text{reject} & \text{otherwise} \end{cases}$$

   Show that both ciphers are not AE-secure.

2. Is group under addition Z_6 a cyclic group? If yes, then please give the generator, and list all the subgroups and their corresponding generators.

3. Is group under multiplication Z_{13}^* a cyclic group? If yes, then please give the generator, and list all the subgroups and their corresponding generators.