Blockchain Technology Fall, 2023
Tutorial 3, Week 5 (Oct 10)
Due Date: Oct 18

Questions:

1. El Gamal Encryption scheme is not CCA-secure. Could you give an attacker that wins the CCA game against the El Gamal Encryption scheme with non-negligible advantage? **(50 points)**

2. Prove that if a hash function is collision-resistant, then it is target-collision-resistant, and if a hash function is target-collision-resistant, then it is preimage-resistant.**(50 points)**