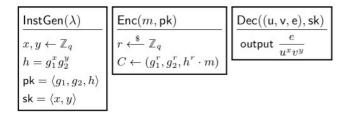
Problem 1

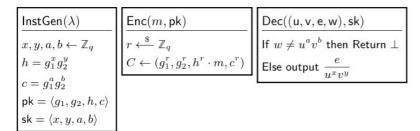
We define the modified ElGamal scheme as follows; given a group \mathcal{G} (of order q with generators g_1, g_2), where the DDH assumption holds, the scheme consists of the following algorithms:



Prove that the scheme is CPA-secure under the DDH assumption.

Problem 2

The simplified Cramer-Shoup scheme is defined, given a group \mathcal{G} (of order q with generators g_1, g_2), where the DDH assumption holds



Prove that the scheme is CCA1-secure under the DDH assumption and show that it is not CCA2-secure.

In a non-adaptive chosen-ciphertext attack (CCA1-security), the adversary is only allowed to query the decryption oracle in the first stage (i.e., before being given the challenge ciphertext c^*). On the other hand, in an adaptive chosen-ciphertext attack (CCA2-security), the adversary is allowed to query the decryption oracle even after the reception of the challenge ciphertext c^* (but it cannot query the oracle on c^*).