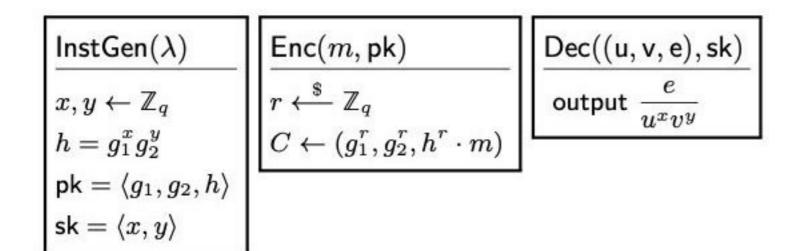
## Problem 1

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.

2020

## Problem 2

Given a group  $\mathcal{G}$ , of order q with generators  $g_1$  and  $g_2$ , we define the simplified Cramer-Shoup scheme as follows.

In the CCA-1 security game, the adversary is allowed to query the decryption oracle only up until it receives the challenge ciphertext. In the adaptive definition (CCA-2), the adversary may continue to query the decryption oracle even after it has received a challenge ciphertext, with the caveat that it may not pass the challenge ciphertext for decryption (otherwise, the definition would be trivial).

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