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:

$\mathsf{InstGen}(\lambda)$	$\mathsf{Enc}(m, \mathsf{pk})$	$\mathsf{Dec}((\mathsf{u}, \mathsf{v}, \mathsf{e}), \mathsf{sk})$
$x, y \leftarrow \mathbb{Z}_q$ $h = g_1^x g_2^y$ $\mathsf{pk} = \langle g_1, g_2, h \rangle$ $\mathsf{sk} = \langle x, y \rangle$	$r \xleftarrow{\$} \mathbb{Z}_q$ $C \leftarrow (g_1^r, g_2^r, h^r \cdot m)$	output $\dfrac{e}{u^x v^y}$

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

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.

$\mathsf{InstGen}(\lambda)$	$\mathsf{Enc}(m, \mathsf{pk})$	$\mathsf{Dec}((\mathsf{u}, \mathsf{v}, \mathsf{e}, \mathsf{w}), \mathsf{sk})$
$x, y, a, b \leftarrow \mathbb{Z}_q$ $h = g_1^x g_2^y$ $c = g_1^a g_2^b$ $\mathsf{pk} = \langle g_1, g_2, h, c \rangle$ $\mathsf{sk} = \langle x, y, a, b \rangle$	$r \xleftarrow{\$} \mathbb{Z}_q$ $C \leftarrow (g_1^r, g_2^r, h^r \cdot m, c^r)$	If $w \neq u^a v^b$ then Return $\perp$ Else output $\dfrac{e}{u^x v^y}$

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.