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:

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

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

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

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^*).