Problem 9): To begin, consider an arbitrary cyclic group $\mathbb{G}$ and a generator $g \in \mathcal{G}$. Then, given any two group elements h_1 and h_2, we define the function $\mathsf{DH}(h_1, h_2)$ as

$$\mathsf{DH}(h_1, h_2) = g^{\log_g h_1 \cdot \log_g h_2} \tag{9.1}$$

The ***DDH*** *Assumption* is that the result of $\mathsf{DH}(h_1, h_2)$, on any uniform group elements h_1 and h_2, is indistinguishable from any other uniform element of the group.

Now, we define the ***El Gamal*** *encryption* algorithm according to

- *Accept input public key* $pk = \langle \mathbb{G}, q, g, h \rangle$.
- *Chose* $y \leftarrow \mathbb{Z}_q$
- *Output the cipher text* $c = \langle c_1, c_2 \rangle$ *determined according to*

$$c = \langle c_1, c_2 \rangle = \langle g^y, h^y \cdot m \rangle$$

We also note that the ***El Gamal*** *encryption* algorithm uses the private key $sk = \langle \mathbb{G}, q, g, x \rangle$. Where $(\mathbb{G}, q, g,)$ is obtained from a generator and h is defined $h \equiv g^x$. Therefore, cipher-text may be encrypted according to the relation

$$\text{For cipher-text } c = \langle c_1, c_2 \rangle \text{ decrypt using } \boxed{m \equiv \frac{c_2}{c_1^x}}$$