1. Consider the following problem: a decryption box, that is given two ciphertexts that encrypt two strings is supposed to decrypt them, order them according to their lexicographic order and present them to a judge. Specifically given any $c_0 = \text{Enc}(m_0), c_1 = \text{Enc}(m_1)$ the decryption box should provide as output to the judge either $(m_0, m_1)$ or $(m_1, m_0)$ depending on the lexicographic order of $m_0, m_1$. How does the judge know that the decryption is correct and that both ciphertexts were decrypted by the decryption box (this would protect the judge against a misbehaving box). On the other hand, the decryption box is only supposed to reveal to the judge the two plaintexts in lexicographic order (and no other information). The judge knows the two ciphertexts $c_0, c_1$ as well as the public-key of the encryption $pk$. Note that the decryption box or the judge does not necessarily trust that the entity that computes the ciphertexts behaves in a reliable way. Describe in detail a protocol between the decryption box and the judge that solves the above problem, based on ElGamal encryption.