Let $G$ be a group with a generator $g$.

1. Construct a sigma protocol for a proof of knowledge of $x$ for a public $y_1 = g^x$ and $y_2 = g^{x^2}$. Prove that the protocol is complete, specially sound, and special honest-verifier zero-knowledge. Implementation is not required. (3pt)

2. Construct a sigma protocol to show that lifted Elgamal ciphertext encrypts a message in range 0 to 7. More precisely, for a public ciphertext $C = (g^m h^r, g^r)$ protocol should prove knowledge of $m$ such that $m \in \{0, 1, \ldots, 7\}$. Describe the protocol and implement it. Proof is not required, but the protocol should be secure. (5pt)

Hint: Encrypt $m$ bitwise and use homomorphic properties.