Q1: Definition of semantic security: describe (briefly) the IND-CPA game

Q2: Identify a flaw (with an explicit example of attack) for the following mutual authentication protocol based on a shared secret K: