3. 다음은 4.2 절에서 살펴본 신뢰하는 키 분배 서버를 이용하는 키 확립 프로토콜이다.

$$\begin{array}{lll} \text{Msg 1.} & A \rightarrow S: & A, B \\ \text{Msg 2.} & S \rightarrow A: & \{B||T_S||K_{AB}\}.K_{AS}, \{A||T_S||K_{AB}\}.K_{BS} \\ \text{Msg 3.} & A \rightarrow B: & \{A||T_S||K_{AB}\}.K_{BS}, \{A||T_A\}.K_{AB} \\ \text{Msg 4.} & B \rightarrow A: & \{T_B||B\}.K_{AB} \end{array}$$

여기서 T_X는 참여자 X가 포함한 현재 시각을 나타내는 타임스템프이다. 이와 관련하여 다음 각각에 대해 답변하시오.

① A와 B는 수신한 키 K_{AB}가 이번 요청을 위해 새롭게 생성한 키임을 어떤 조건 하에 확신을 가질 수 있는지 설명하시오.

② A와 B는 상대방이 자신과 같은 키를 가지고 있는지 확신할 수 있는지 설명하시오.

③ 그림 4.5의 프로토콜과 비교하여 차이점을 설명하시오.

A - 1. 메시지 2의 경우, 타임스템프가 포함되어있기 때문에 새롭게 생성한 키임을 확신할 수 있다.

A - 2. 알 수 없다.

A - 3. A와 B가 서로 같은 키를 가졌다는 것을 확인할 수 없다는 차이가 있다.

4. 다음과 같은 간단한 프로토콜을 생각하여 보자.

$$\begin{array}{lll} \text{Msg 1.} & A \rightarrow B: & \{N_A\}.+K_B \\ \text{Msg 2.} & B \rightarrow A: & N_A \end{array}$$

이와 관련하여 다음 각각에 대해 답변하시오.

① A는 메시지 2에서 N_A를 수신하면 무엇을 확신할 수 있는지 설명하시오.

② 2번 메시지를 $\text{Sig}_B(A||N_A)$로 변경하면 A는 이를 통해 무엇을 확신할 수 있는지 설명하시오.

A - 1. A가 사용한 공개키가 B의 공개키임을 확신할 수 있다.

A - 2. 메시지를 주고받는 상대가 B임을 확신할 수 있다.