Ans 1) 공격자는 예측한 난스값을 이용해서 K_{AB}값을 계산할 수 있다. 이를 통해 이후의 ㅁ든 통신에 대하여, 공격자는 모든 통신을 가로챌 수 있게 된다. 이는 메시지 무결성과 기밀성을 보장하지 못한다는것을 의미한다. 또한, 이 프로토콜에서는 메시지 인증이 이루어지지 않기 때문에 A, B는 이를 감지하지 못한다는것을 이용하여 공격자는 메시지를 변조하여 전송할 수 있다.

Ans 2) 각 방향마다 다른 키를 사용하는 경우, 공격자는 KAB를 알지 못하기 때문에 타입 공격이 불가능하다. 따라서 각 방향마다 다른 키를 사용하는것은 보안성을 향상시키는데 도움이 된다.

Ans 3) 이 프로토콜에서는 각 방향마다 다른 키를 사용하지 않기 때문에 타입 공격이 가능하다. 메시지 1과 4에서 A와 B의 값은 이미 알려져 있기 때문에, 공격자는 {NA||KAB}.KAS를 복호화 하여 KAB를 알아낼 수 있다. 이후 공격자는 KAB를 이용하여 NA, N, A, B의 값을 알아낼 수 있고, 메시지 2에서 NB값을 알아낼 수 있다. 마지막으로 메시지 3에서 KAB의 값을 확인할 수 있다. ECB모드의 경우, 블록 암호에서 중복되는 평문 블록을 동일한 암호화 블록으로 변환하기 때문에 보안성이 낮다. 따라서 공격자는 암호화된 메시지의 구조를 알아낼 수 있고, 원하는 내용을 임의로 조작할 수 있기 때문에 타입 공격이 가능하다.

Ans 4) 그림 7.6의 경우, a가 노출되었을 때, 재전송 공격이 가능하다. 공격자는 이전에 수신한 메시지 2를 그대로 재전송 하면 된다. 이 경우, 공격자는 B의 개인키인 b을 얻고, 이를 이용하여 SAB를 계산할 수 있다.
그림 7.7의 경우 a가 노출된다고 하더라도 재전송 공격이 불가능하다. 그 이유는 g^a와 g^b를 제외한 나머지의 값들이 매번 다르기 때문이다. 따라서 재전송 공격을 하더라도 SAB와 SBA를 구할 수 없다.
그림 7.8의 경우에서도 a가 노출된다고 하더라도 재전송 공격이 불가능하다. 이 프로토콜에서는 B가 g^a, g^b, A의 서명을 A에게 전송하지만, 이 서명은 g^a, g^b, A의 조합에 대해서만 유효하기 때문에, 이를 공격자가 그대로 전송하더라도 재전송 공격이 불가능하다.