Etude de protocoles d'authentification (partie 2)

Protocole 1

1. $A \rightarrow B : A, N_A$
2. $B \rightarrow A : \{N_A, K'_{AB}\}K_{AB}$
3. $A \rightarrow B : \{N_A\}K'_{AB}$
4. $B \rightarrow A : N'_B$

Questions :
-Traduisez le protocole tel qu'il est écrit en notation de protocole de sécurité dans des phrases en langue naturelle expliquant son déroulement.
-Essayez de trouver une attaque contre ce protocole où l'attaquant réussi à mener deux sessions parallèles avec *A* en souhaitant se faire passer pour *B*. Dans la première session A est l'initiateur de la session alors que dans l'autre l'attaquant est l'initiateur de cette session.
-Comment peut-on modifier le protocole pour se prémunir contre cette attaque?

Protocole 2

1. $A \rightarrow B : A$
2. $B \rightarrow A : N_B$
3. $A \rightarrow B : \{N_B\}K_{AS}$
4. $B \rightarrow S : \{A, \{N_B\}K_{AS}\}K_{BS}$
5. $S \rightarrow B : \{N_B\}K_{BS}$

Questions :
-Traduisez le protocole tel qu'il est écrit en notation de protocole de sécurité dans des phrases en langue naturelle expliquant son déroulement.
-Essayez de trouver une attaque contre ce protocole où l'attaquant réussi à mener deux sessions parallèles avec *B*. Dans la première session l'attaquant est l'initiateur de la session et se fait passer pour A alors que dans l'autre l'attaquant est aussi l'initiateur de cette session mais il ne cache pas son identité.
-Comment peut-on modifier le protocole pour se prémunir contre cette attaque?