Solution exercice devoir SecInf:

En se basant sur les notations suivantes l'exercice 4 (TD1), donnez la spécification des protocoles de sécurité suivants :

1. Les communications entre Alice te Bob doivent être authentifiées (donner les deux réponses possibles)
   Authentification asymétrique :
   A =>B : M . { H(M) } Ska
   B=>A : M . {H (M)} SKb
   Authentification symétrique
   A=>B ou B=>A : {Kab} PKb . {H(Kab)} SKa
   A =>B : M . H_k (M)
   B=>A : M . H_k (M)
2. Les communications entre Alice et Bob doivent être confidentielles (donnez les deux solutions possibles puis, indiquez laquelle est plus avantageuse).
   Confientialité asymétrique :
   A=>B : {M} PKb
   B=>A : {M} PKa
   Confientialité symétrique (plus avantageuse) :
   A=>B ou B=>A : {Kab} PKb . {H(Kab)} SKa
   A=>B : {M} Kab
   B=>A: {M} Kab
3. Seulement les flux de communication destinés à Bob qui doivent être sécurisés (services nécessaires : confidentialité symétrique, non-répudiation et intégrité).
   A=>B: {Kab} PKb . {H(Kab)} SKa
   A=>B : {M} Kab . {H(M)} SKa