MEVS 2009-2010 **Exercices**

Modélisation des protocoles en clauses de Horn

Exercice 1 *Le protocole d'Otway Rees est décrit par la séquence suivante :*

1. $A \longrightarrow B : M, A, B, \{Na, M, A, B\}_{Kas}$
2. $B \longrightarrow S : M, A, B, \{Na, M, A, B\}_{Kas}, \{Nb, M, A, B\}_{Kbs}$
3. $S \longrightarrow B : M, \{Na, Kab\}_{Kas}, \{Nb, Kab\}_{Kbs}$
4. $B \longrightarrow A : M, \{Na, Kab\}_{Kas}$

On suppose que

- *S est un serveur de distribution de clé*
- *M, Na et Nb sont des nonces*
- *Kij dénote la clé partagée entre I et J*
- *Kab est une clé fraîchement générée*

Donnez une modélisation en clauses de Horn

- *des capacités de l'intrus;*
- *du protocole.*

Exercice 2 *Soit l'ensemble de clauses de Horn B_0 suivant:*

$$\begin{array}{rcll} I(x), I(y) & \rightarrow & I(\langle x, y\rangle) & (1) \\ I(a[]), I(b[]) & \rightarrow & I(\langle a[], b[]\rangle) & (2) \\ & \rightarrow & I(pk(ska[])) & (3) \\ I(pk(x)) & \rightarrow & I(\{N[x]\}_{pk(x)}) & (4) \end{array}$$

Quel est l'ensemble de clauses B' calculé par la phase 1 de l'algorithme de résolution donné en cours si $S = I(x)$.