MEVS 2009-2010 **Exercices**

Termes et déduction

Exercice 1 *Est-ce que les paires de termes suivantes sont unifiables. Si c'est le cas donnez l'unificateur le plus général.*

- $\langle x, y\rangle$, $\langle a, z\rangle$
- $\langle x, y\rangle$, $\langle a, \langle b, c\rangle\rangle$
- $\langle a, b\rangle$, $\{x\}_y$
- $\langle \{a\}_x, x\rangle$, $\langle \{a\}_b, a\rangle$
- x, $\langle \{y\}_b, a\rangle$

Exercice 2 *Soit le terme* $t = \langle \{s\}_{\langle k_1,k_2\rangle}, \langle \{k_2\}_{k_1}, k_2\rangle\rangle$.

1. *Donnez* $t|_{212}$. *Quels sont les positions et sous-termes de* t *?*
2. *Quelle est la taille de* t *? Quelle est la taille DAG de* t *?*

Exercice 3 *Considérons le système d'inférence* $\mathcal{I}_{DY}$

$$\frac{x \quad y}{\langle x, y\rangle} \qquad \frac{x \quad y}{\{x\}_y} \qquad \frac{\langle x, y\rangle}{x} \qquad \frac{\langle x, y\rangle}{y} \qquad \frac{\{x\}_y \quad y}{x}$$

1. *Montrez que* $\{\{s\}_{\langle k_1,k_2\rangle}, \langle \{k_2\}_{k_1}, k_1\rangle\} \vdash_{\mathcal{I}_{DY}} s$ *en donnant l'arbre de dérivation.*
2. *Montrez que* $\{\{s\}_{\langle k_1,k_2\rangle}, k_2\} \nvdash_{\mathcal{I}_{DY}} s$.

Exercice 4 *Soit le protocole suivant :*

$$A \to B : \ \langle \{k_1\}_{k_2}, m\rangle$$
$$B \to A : \ \{m\}_{\langle k_1,k_2\rangle}$$

On suppose que k_2 *est une clé partagée par* A *et* B. *Montrez que* k_1 *reste secret en présence d'un attaquant Dolev-Yao passif qui ne connaît ni* m, *ni* k_1, *ni* k_2.

Exercice 5 *On propose la procédure suivante pour décider si* $\{t_1, \ldots, t_n\} \vdash_{\mathcal{I}_{DY}} t$*:*

1. *Appliquer les règles* $\dfrac{\{x\}_y \quad y}{x}$ *et* $\dfrac{\langle x_1, x_2\rangle}{x_i}$ *jusqu'à obtenir un point fixe.*
2. *Essayer de construire* t *à partir de l'ensemble des termes obtenus ci-dessous en utilisant uniquement les règles* $\dfrac{x \quad y}{\{x\}_y}$ *et* $\dfrac{x_1 \quad x_2}{\langle x_1, x_2\rangle}$.

Pourquoi cette procédure est-elle fausse ?
Quelle restriction supplémentaire faudrait-il pour qu'elle soit correcte ?

Exercice 6 *Donnez un exemple de système d'inférence pour lequel on n'a pas la propriété de localité.*