

Exercice 1

On considère le protocole suivant :

$$\begin{aligned} A \rightarrow B & : \{\{K\}_{\text{pub}(B)}, A\}_{\text{pub}(B)} \\ B \rightarrow A & : \{\{K\}_{\text{pub}(A)}, B\}_{\text{pub}(A)} \end{aligned}$$

Le but de ce protocole est que les agents A et B établissent une clef de session. Celle-ci doit rester secrète entre A et B . Pour cela, A envoie à B une nouvelle clef de session K en utilisant du chiffrement asymétrique et la clef publique de B . L'agent B répond à A pour lui signaler qu'il a bien réceptionné cette nouvelle clef K . À partir de là, on peut imaginer que les agents A et B utilisent cette clef K et le chiffrement symétrique pour communiquer.

Montrer que ce protocole peut-être attaqué.

Exercice 2 (*plus difficile*)

On considère une variante du protocole de Needham-Schroeder. Ce protocole est le suivant :

$$\begin{aligned} A \rightarrow B & : \{A, N_a\}_{\text{pub}(B)} \\ B \rightarrow A & : \{N_a, N_b, B\}_{\text{pub}(A)} \\ A \rightarrow B & : \{N_b\}_{\text{pub}(B)} \end{aligned}$$

1. Vérifier que l'attaque « man-in-the-middle » précédent n'existe plus.
2. Montrer qu'il existe à nouveau une attaque sur N_b .
Indication : attaque par confusion de type
3. Cette attaque vous semble-t-elle réaliste ?

D'autres exemples sont disponibles à l'adresse <http://www.lsv.ens-cachan.fr/spore/table.html>.

Exercice 3

Dire si les couples de termes suivants sont unifiables. Si oui, donner un unificateur.

1. $\langle x, b \rangle$ et $\langle a, y \rangle$,
2. $\{x\}_{\text{pub}(a)}$ et $\{b\}_{\text{pub}(x)}$,
3. $\langle x, y \rangle$ et $\langle h(y), a \rangle$,
4. z et $\langle x, y \rangle$.

Exercice 4

On considère le système d'inférence suivant :

$$\frac{T \vdash u \quad T \vdash v}{T \vdash \langle u, v \rangle} \quad \frac{T \vdash u \quad T \vdash v}{T \vdash \{u\}_v} \quad \frac{T \vdash \langle u, v \rangle}{T \vdash u} \quad \frac{T \vdash \langle u, v \rangle}{T \vdash v} \quad \frac{T \vdash \{u\}_v \quad T \vdash v}{T \vdash u}$$

Soit $T = \{\{s\}_{\langle k_1, k_2 \rangle}, \{k_1\}_{k_3}, k_3, k_2\}$.

1. Énumérer les sous-termes de T .

2. Le terme s est déductible de T . Donner une dérivation.
3. Parmi les sous-termes de T quels sont les sous-termes déductibles ?
4. Donner un terme déductible qui n'est pas un sous-terme.

Exercice 5 (*plus difficile*)

On considère le système d'inférence de l'exercice précédent. Pour décider si un terme s est déductible à partir d'un ensemble de termes T , on propose l'algorithme suivant :

Algorithme :

1. appliquer le plus possible les règles de projection et de déchiffrement,
2. essayer de construire s en appliquant les règles de *synthèse* : application du chiffrement et de la paire.
1. Montrer que cet algorithme termine.
2. Montrer que l'algorithme est correct, i.e. si l'algorithme arrive à construire s alors s est déductible à partir de T .
3. L'algorithme n'est pas complet. Il se peut que le terme s soit déductible et que l'algorithme ne réussisse pas à construire s . Trouver un exemple illustrant cette situation.
4. Quelle hypothèse faudrait-il ajouter pour avoir un algorithme complet ?
5. Montrer la complétude de l'algorithme sous cette hypothèse.

Exercice 6

On considère le système d'inférence suivant permettant de modéliser le chiffrement asymétrique.

$$\frac{T \vdash u \quad T \vdash v}{T \vdash \{u\}_v} \quad \frac{T \vdash \{u\}_{\text{pub}(v)} \quad T \vdash \text{prv}(v)}{T \vdash u} \quad \frac{T \vdash u}{T \vdash \text{pub}(u)}$$

1. Ce système est-il local ? Si oui, montrez-le. Si non, donnez une dérivation montrant qu'il ne l'est pas.

Exercice 7 (*plus difficile*)

On considère le système d'inférence suivant permettant de modéliser la signature.

$$\frac{T \vdash u \quad T \vdash \text{prv}(v)}{T \vdash \text{sign}(u, \text{prv}(v))} \quad \frac{T \vdash \text{sign}(u, \text{prv}(v)) \quad T \vdash \text{pub}(v)}{T \vdash u} \quad \frac{T \vdash u}{T \vdash \text{pub}(u)}$$

1. Ce système n'est pas local pour la notion de sous-terme utilisé en cours. Donnez un contre-exemple.
2. Montrer que le problème de déduction est quand même décidable.
On utilisera la technique vu en cours en utilisant une notion de sous-terme étendue.