Vérification automatique de protocoles cryptographiques
Sujet de réflexion pour la première partie de l'examen

19 mars 2003

On suppose ici que

$$\{< u, v >\}_k =< \{u\}_k, \{v\}_k >$$

ce qui est censé modèliser un chiffrement par blocs.

Cette équation peut être orientée de gauche à droite en un système de réécriture convergent (admis), si bien que tout terme u construit à l'aide de la paire, du chiffrement et de constantes a une unique forme normale $u \downarrow$. On considère alors les règles de déduction de l'intrus de Dolev-Yao dans lesquelles la règle de chiffrement est remplacée par :

$$\frac{T \vdash u \quad T \vdash v}{T \vdash \{u\}_v \downarrow}$$

On se propose de démontrer des résultats analogues à ceux qu'on a obtenu en cours pour le modèle de Dolev-Yao, avec ce nouveau modèle de déduction de l'intrus. Pour simplifier, on ne considèrera que des clefs symétriques.

Pour tout ensemble fini de termes clos T, soit $St(T)$ l'ensemble des sous-termes des termes de T et soit $S(T)$ le plus petit ensemble de termes tel que

- $T \subseteq S(T)$
- $St(S(T)) \subseteq S(T)$
- Si u, v sont en forme normale et $\{u\}_v \downarrow \in S(T)$, alors $u \in S(T)$.

La taille d'un ensemble fini de termes T est le cardinal de $St(T)$.

Lemme

Si T est un ensemble fini de termes clos en forme normale, alors $S(T)$ est de taille polynômiale dans la taille de T.

Squelette de la première partie de l'examen

Les questions sont volontairement imprécises. Elles seront précisées le 26 mars.

1. Donner un exemple de protocole qui montre les différences entre ce modèle d'intrus et le modèle de Dolev-Yao
2. (question facultative) démontrer le lemme
3. En s'inspirant du cours et à l'aide du lemme, donner un algorithme de faible complexité qui, étant donnés T et u (termes en forme normale), décide si $T \vdash u$ est dérivable.