

F. Autreau
P. Lafourcade
JL. Roch

P. Lafourcade.

SET 5

Date: 05.17.2008

Exercise 1

Let T be a set of terms. The mapping $S : T \rightarrow T$. Prove that

1. $S(A \cup B) = S(A) \cup S(B)$
2. S is idempotent: $S(S(A)) = S(A)$
3. S is monotonous: if $A \subseteq B$ then $S(A) \subseteq S(B)$
4. S is transitive: if for all $X, Y, Z \subseteq T$, $X \subseteq S(Y)$ and $Y \subseteq S(Z)$ implies $X \subseteq S(Z)$.

Exercise 2

If P is a minimal proof of $T \vdash u$ then P is a simple proof of $T \vdash u$.

Exercise 3

Is it possible from T_0 to deduce s

- $T_0 = \{a, k\}$ and $s = \langle a, \{a\}_k \rangle$
- $T_0 = \{\{k\}_a, b\}$ and $s = \langle \{b\}_{\{k\}_a}, \{k\}_a \rangle$
- $T_0 = \{\langle a, \{k\}_a \rangle\}$ and $s = \{\langle a, \{k\}_a \rangle\}_k$
- $T_0 = \{a, k\}$ and $s = \langle b, \{k\}_a \rangle$

Exercise 4

Consider the following protocol:

$$\begin{aligned} A \rightarrow B &: \langle \{k_1\}_{k_2}, m \rangle \\ B \rightarrow A &: \{m\}_{\langle k_1, k_2 \rangle} \end{aligned}$$

Assume that k_2 is a shared key between A and B . Show that k_1 is secret in presence of passive Dolev-Yao intruder.

Exercise 5

Give an exemple of inference system for which the locality property is false.