SET 2
Date: 11.10.2007

Exercise 1

$S(t)$ is the smallest set such that:

- $t \in S(t)$
- $\langle u, v \rangle \in S(t) \Rightarrow u, v \in S(t)$
- $\{u\}_v \in S(t) \Rightarrow u, v \in S(t)$

(A) $\frac{u \in T_0}{T_0 \vdash u}$

(UL) $\frac{T_0 \vdash \langle u, v \rangle}{T_0 \vdash u}$

(P) $\frac{T_0 \vdash u \quad T_0 \vdash v}{T_0 \vdash \langle u, v \rangle}$

(UR) $\frac{T_0 \vdash \langle u, v \rangle}{T_0 \vdash v}$

(C) $\frac{T_0 \vdash u \quad T_0 \vdash v}{T_0 \vdash \{u\}_v}$

(D) $\frac{T_0 \vdash \{u\}_v \quad T_0 \vdash v}{T_0 \vdash u}$

We denote $S'(t) = \{ t \mid p \in Pos(t) \}$ the set of subterms of $t$.

Prove that $S'(t) = S(t)$

Exercise 2

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 monotonus: 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 3

If $P$ is a minimal proof of $T \vdash u$ then $P$ is a simple proof of $T \vdash u$. 
Exercise 4
We propose the following procedure to know if \( \{t_1, \ldots, t_n\} \vdash_{IY} t \):

1. Apply first the rules decomposition \((D), (UR), (UL)\):

\[
\begin{align*}
\text{(UL)} & \quad T_0 \vdash \langle u, v \rangle \\
\text{(UR)} & \quad T_0 \vdash u \\
\text{(D)} & \quad T_0 \vdash \{u\}_v \\
& \quad T_0 \vdash u
\end{align*}
\]

until to reach a fix point.

2. Try to build \( t \) from this new set of terms using only composition rules \((P), (C)\):

\[
\begin{align*}
\text{(P)} & \quad T_0 \vdash u \\
\text{(C)} & \quad T_0 \vdash \{u\}_v
\end{align*}
\]

Why this procedure is false?
What is the restriction we have to add to get this result true?

Exercise 5
Consider the following protocol:

\[
A \rightarrow B : \langle \{k_1\}_{k_2}, m \rangle \\
B \rightarrow A : \{m\}_{(k_1,k_2)}
\]

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 6
Give an exemple of inference system for which the locality property is false.

Exercise 7
Find an attack using a passive intruder against Shamir 3-Pass Protocol if we used Vernam encryption.

\[
\begin{align*}
1 & \quad A \rightarrow B : \{m\}_{K_A} \\
2 & \quad B \rightarrow A : \{m\}_{K_A} \{m\}_{K_B} = \{m\}_{K_B} \{m\}_{K_A} \\
3 & \quad A \rightarrow B : \{m\}_{K_B}
\end{align*}
\]