Exercices

Exercise 1

- Solve the following syntactic unification problems. If there is no unifier, explain why

  1. $f(x,y) \stackrel{?}{=} f(h(a),x)$
  2. $f(x,y) \stackrel{?}{=} f(h(x),x)$
  3. $f(x,a) \stackrel{?}{=} f(h(b),b)$
  4. $f(x,x) \stackrel{?}{=} f(h(y),y)$

- Now solve each of the above, modulo commutativity of f, i.e. $\forall x, y \quad f(x,y) = f(y,x)$.

Exercise 2

We recall the rules of the Deduction System for Dolev Yao theory: $T_0 \vdash s$, where $[\![ ]\!]_{\_}$ represents a symmetric encryption scheme, $\{\ \_\ \}_{\_}$ an asymmetric encryption scheme, and we suppose that $pr(u)$ is the inverse secret key associated to $pk(u)$:

$$(\mathbf{A}) \quad \frac{u \in T_0}{T_0 \vdash u} \qquad\qquad (\mathbf{UL}) \quad \frac{T_0 \vdash \langle u, v\rangle}{T_0 \vdash u}$$

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

$$(\mathbf{C}) \quad \frac{T_0 \vdash u \qquad T_0 \vdash v}{T_0 \vdash [\![u]\!]_v} \qquad\qquad (\mathbf{D}) \quad \frac{T_0 \vdash [\![u]\!]_v \qquad T_0 \vdash v}{T_0 \vdash u}$$

$$(\mathbf{AD}) \quad \frac{T_0 \vdash \{\ u\ \}_{pk(v)} \qquad T_0 \vdash pr(v)}{T_0 \vdash u} \qquad\qquad (\mathbf{AC}) \quad \frac{T_0 \vdash u \qquad T_0 \vdash pk(v)}{T_0 \vdash \{\ u\ \}_{pk(v)}}$$

The set of **Syntactic Subterms** of a term t, denoted by $S(t)$, is the smallest set such that:

- $t \in S(t)$
- $\langle u, v\rangle \in S(t) \Rightarrow u, v \in S(t)$
- $[\![u]\!]_v \in S(t) \Rightarrow u, v \in S(t)$

For a set T of terms, we define $S(T) = \bigcup_{t \in T} S(t)$.

The following algorithm allows to decide if $T_0 \vdash w$ (where $T \vdash^{\leq 1} s$ means that s can be obtained from T using only one rule from the Deduction System):

McAllester's Algorithm

Input : T_0, w

$\quad T \leftarrow T_0$;

$\quad$ while ($\exists s \in S(T_0 \cup \{w\})$ such that $T \vdash^{\leq 1} s$ and $s \notin T$)

$\quad\quad T \leftarrow T \cup \{s\}$;

Output :$w \in T$

Using the above algorithm, prove or disprove that a passive Dolev Yao intruder can deduce the message s with the initial knowledge T_0.

1.) $T_0 = \{a, k\}$ and $s = \langle a, \{\!\{a\}\!\}_k \rangle$

2.) $T_0 = \{a, k, n1, \{\!\{k2\}\!\}_{\langle n1, n2 \rangle}, \{\!\{\langle n2, \{\!\{n1\}\!\}_{\langle n3, n3 \rangle} \rangle\}\!\}_k\}$ and $s = k2$

3.) $T_0 = \{a, b, k1, k2, \{\!\{k4\}\!\}_{\langle k1, k3 \rangle}, \{\!\{\langle k2, n \rangle\}\!\}_{\langle k2, k1 \rangle}, \{\!\{\langle k2, k3 \rangle\}\!\}_{\langle k4, k1 \rangle}\}$ and $s = k4$

Exercise 3

Consider the following protocol:

$$\begin{array}{llcll} 1. & A & \rightarrow & B & : \boldsymbol{\{} \langle A, N_a \rangle \boldsymbol{\}}_{pk(B)} \\ 2. & B & \rightarrow & A & : \langle \boldsymbol{\{} \langle A, K \rangle \boldsymbol{\}}_{pk(A)}, \{\!\{N_a\}\!\}_K \rangle \\ 3. & A & \rightarrow & B & : \boldsymbol{\{} \langle \langle A, B \rangle, K \rangle \boldsymbol{\}}_{pk(B)} \end{array}$$

Assume that $\boldsymbol{\{}\ \_\ \boldsymbol{\}}_{\_}$ is an asymmetric encryption scheme, $pk(x)$ (respectively $pr(x)$) is the public key (respectively private key) of participant x.

1. Consider a session between two honest participants a and b and show that k (the instantiation of variable K in this session) remains secret in presence of a passive Dolev-Yao intruder.

2. We assume now that the adversary i is active (he controls the network).

    1.) Consider the scenario corresponding to a session of a as initiator with i, and to a session of b as responder.

    Suppose that the initial knwoledge of the intruder i is the set $T_1 = \{a, b, pk(a), pk(b), pk(i), pr(i)\}$, i.e. we suppose that a and b are honest. Suppose that at the end, b will think that he is talking and sharing a secret value k with a. Can you find an attack where the intruder i will learn k?

    2.) Can you correct the protocol? Justify your answer.

Exercise 4

Consider the following (Needham-Schroeder-Lowe) protocol:

$$\begin{array}{llcll} 1. & A & \rightarrow & B & : \boldsymbol{\{} \langle A, N_a \rangle \boldsymbol{\}}_{pk(B)} \\ 2. & B & \rightarrow & A & : \boldsymbol{\{} \langle N_a, \langle N_b, B \rangle \rangle \boldsymbol{\}}_{pk(A)} \\ 3. & A & \rightarrow & B & : \boldsymbol{\{} N_b \boldsymbol{\}}_{pk(B)} \end{array}$$

Assume that $\{\!\!\{ \_ \}\!\!\}_{\_}$ is an asymmetric encryption scheme, $pk(x)$ (respectively $pr(x)$) is the public key (respectively private key) of participant x. This protocols ensures secrecy of N_b, and injective agreement from the perspective of both the initiator and the responder. Show that the following modified version of Needham-Schroeder-Lowe protocol:

$$\begin{array}{llll} 1. & A & \rightarrow & B & : \{\!\!\{ \langle A, N_a \rangle \}\!\!\}_{pk(B)} \\ 2. & B & \rightarrow & A & : \{\!\!\{ \langle N_a, N_b \oplus B \rangle \}\!\!\}_{pk(A)} \\ 3. & A & \rightarrow & B & : \{\!\!\{ N_b \}\!\!\}_{pk(B)} \end{array}$$

is not correct. It allows an attack on both the secrecy of N_b and on the authentication of B. This arises because $\oplus$ has algebraic properties that the free algebra assumption ignores: for instance, it is associative, commutative, and has the cancellation property $X \oplus X = 0$. What can you say about the following protocol?

$$\begin{array}{llll} 1. & A & \rightarrow & B & : \{\!\!\{ \langle A, N_a \rangle \}\!\!\}_{pk(B)} \\ 2. & B & \rightarrow & A & : \{\!\!\{ \langle N_a \oplus B, N_b \rangle \}\!\!\}_{pk(A)} \\ 3. & A & \rightarrow & B & : \{\!\!\{ N_b \}\!\!\}_{pk(B)} \end{array}$$

Exercise 5

In this exercice, $(\_, \_)$ represents concatenation, and $\{\_\}_{\_}^{\_}$ represents a probabilistic symmetric encryption scheme (the randomness used is explicit now). We recall that two messages m_0 and m_1 are equivalent in the Dolev Yao model (written $m_0 \sim m_1$) if there is a renaming (a bijection) σ_K of keys of m_1 and a renaming σ_R of random coins of m_1 such that $\mathbf{pat}(m_0) = \mathbf{pat}(m_1)\sigma_K\sigma_R$.

Prove or disprove the symbolic equivalence $\sim$ in the Dolev Yao model of the following pairs of messages $m_0 \overset{?}{\sim} m_1$:

$$\begin{array}{lll} 1.) & m_0 = (\{(1, \{0\}_{k_1}^{r'})\}_k^r, \{0\}_k^{r'}), & m_1 = (\{(1,0)\}_{k_3}^{r'}, \{1\}_{k_3}^s) \\ 2.) & m_0 = ((\{(0, \{1\}_k^{r'})\}_{k_1}^r, \{1\}_k^{r'}), k_1), & m_1 = ((\{(0, \{1\}_k^{r'})\}_{k_1}^r, \{1\}_k^{r''}), k_1) \\ 3.) & m_0 = (\{(0, \{1\}_k^{r'})\}_k^r, \{0\}_{k'}^{r'}), & m_1 = (\{0\}_k^{r'}, \{0\}_k^s) \end{array}$$

Exercise 6

We recall that a family of distributions $\mathcal{E}$ is called **polynomial-time constructible**, if there is a ppt-algorithm $\Psi_{\mathcal{E}}$, such that the output of $\Psi_{\mathcal{E}}(\eta)$ is distributed identically to $\mathcal{E}_\eta$. Given two families of distributions $\mathcal{D}$ and $\mathcal{E}$, we define $\mathcal{D} \| \mathcal{E}$ by

$$(\mathcal{D} \| \mathcal{E})_\eta = [x \leftarrow^R \mathcal{D}_\eta; y \leftarrow^R \mathcal{E}_\eta : \ (x, y)]$$

Prove or disprove the following assertions (where $\approx$ is the computational indistingushability relation over distributions):

- If $\mathcal{D}^0 \approx \mathcal{D}^1$ and $\mathcal{E}^0 \approx \mathcal{E}^1$ and $\mathcal{D}^0, \mathcal{D}^1, \mathcal{E}^0, \mathcal{E}^1$ are all polynomial-time constructible, then $(\mathcal{D}^0 \| \mathcal{E}^0) \approx (\mathcal{D}^1 \| \mathcal{E}^1)$.
- If $(\mathcal{D}^0 \| \mathcal{E}^0) \approx (\mathcal{D}^1 \| \mathcal{E}^1)$ then $\mathcal{D}^0 \approx \mathcal{D}^1$ and $\mathcal{E}^0 \approx \mathcal{E}^1$.

Exercise 7

We use $\oplus$ to denote the usual bitwise xor over equal-length bitstrings, e.g. $0011 \oplus 1110 = 1101$, and $01 \oplus 00 = 01$.

Given two families of distributions $\mathcal{D}$ and $\mathcal{E}$, such that for any η, both $\mathcal{D}_\eta$ and $\mathcal{E}_\eta$ are distributions over strings of length η, we define $\mathcal{D} \oplus \mathcal{E}$ by

$$(\mathcal{D} \oplus \mathcal{E})_\eta = [x \xleftarrow{R} \mathcal{D}_\eta; y \xleftarrow{R} \mathcal{E}_\eta : \ (x \oplus y)]$$

.

Prove or disprove the following assertions (where $\approx$ is the computational indistingushability relation over distributions):

- If $\mathcal{D}^0 \approx \mathcal{D}^1$ and $\mathcal{E}$ is polynomial-time constructible, then $(\mathcal{D}^0 \oplus \mathcal{E}) \approx (\mathcal{D}^1 \oplus \mathcal{E})$.
- If $(\mathcal{D}^0 \oplus \mathcal{E}) \approx (\mathcal{D}^1 \oplus \mathcal{E})$ then $\mathcal{D}^0 \approx \mathcal{D}^1$.