SET 2

Exercise 1
Find a type flaw attack on Yahalom Protocol:
1 \( A \to B : (A, N_A) \)
2 \( B \to S : (B, (A, N_A, N_B)_{K_{bs}}) \)
3 \( S \to A : ((B, Kab, N_A, N_B)_{K_{as}}, (A, Kab, N_B)_{K_{bs}}) \)
4 \( A \to B : ((A, Kab)_{K_{bs}}, (N_B)_{K_{ab}}) \)

Exercise 2
The following protocol, called Andrew Secure RPC, can be used to establish a temporary
session key between parties \( A \) and \( B \) who already share a long-term secret \( K_{ab} \):
1 \( A \to B : \{N_a\}_{K_{ab}} \)
2 \( B \to A : \{N_a + 1, N_b\}_{K_{ab}} \)
3 \( A \to B : \{N_b + 1\}_{K_{ab}} \)
4 \( B \to A : \{K'_{ab}, N'_b\}_{K_{ab}} \)
Show an attack on this protocol. \textit{Hint}: what could an adversary do if he somehow learned
a \( K'_{ab} \) from a previous instance of the protocol?

Exercise 3
Prove or disprove that a passive Dolev Yao intruder can deduce the following messages
with the initial knowledge \( T_1 \), where \( \{.\} \) represents a symmetric encryption scheme.

- \( T_1 = \{m_1, m_2\}, \{m_1, m_4\}\}_{m_3}, m_4, \{m_5\}_{m_4}, m_6, \{m_4, m_7\}\}_{m_6}, m_7 \) and \( s = \{m_1\}_{m_1} \).
- \( T_1 = \{a\}_{k}, \{c\}_{a}, \{k\}_{\{a\}_k} \) and \( s = c. \)
- \( T_1 = \{m_1, m_2\}, \{m_1, m_4\}\}_{m_3}, m_4, \{m_5\}_{m_4}, m_6, \{m_4, m_7\}\}_{m_6}, m_7 \) and \( s = m_3. \)
- \( T_1 = \{m_1, m_2\}, \{m_1, m_4\}\}_{m_3}, m_4, \{m_5\}_{m_4}, m_6, \{m_4, m_7\}\}_{m_6}, m_7 \) and \( s = m_5. \)
- \( T_1 = \{\{k_1\}_{k_2}, m\}, \{m\}_{\{k_1,k_2\}} \) and \( s = k_2. \)
- \( T_1 = \{m_1\}_{m_2}, m_2, \{m_3\}_{m_2,m_4}, \{m_1, m_4\}\}_{m_3,m_4} \) and \( s = \{m_3, m_4\}. \)

Exercise 4 (Final 2007)
Give the mgu between \( t \) and \( s \) for the following terms, where \( x, y, z \) are variables and \( a, b \)
constants:
Exercise 5 (Final 2007)
Prove or disprove that a passive Dolev Yao intruder can deduce the following messages with the initial knowledge $T_1$, where $\{\cdot\}$ represents a symmetric encryption scheme.

- $T_1 = \{(m_1,m_2), \{m_1,m_4\}_{m_3}, m_4, \{m_5\}_{m_4}, m_6, \{(m_4,m_7)\}_{m_6}, m_7\}$ and $s = \{m_1\}_{m_1}$.
- $T_1 = \{\{a\}_k, \{c\}_a, \{k\}_{\{a\}_k}\}$ and $s = c$.
- $T_1 = \{(m_1,m_2), \{m_1,m_4\}_{m_3}, m_4, \{m_5\}_{m_4}, m_6, \{(m_4,m_7)\}_{m_6}, m_7\}$ and $s = m_5$.
- $T_1 = \{\{\{k_1\}_k, m\}, \{m\}_{\{k_1,k_2\}}\}$ and $s = k_2$.

Exercise 6 (Final 2009)
We recall the Yahalom protocol, where $Kas$, $Kbs$ and $Kab$ are symmetric keys.

1. $A \to B$: $A, N_A$
2. $B \to S$: $B, \{A, N_A, N_B\}_{Kbs}$
3. $S \to A$: $\{B, Kab, N_A, N_B\}_{Kas}, \{A, Kab\}_{Kbs}$
4. $A \to B$: $\{A, Kab\}_{Kbs}, \{N_B\}_{Kab}$

1. Give a role description of this protocol.
2. Give a constraint system associated to your role description.
3. Propose a type flaw attack on this protocol.
   Hint: message 3 is not used in the attack.

Exercise 7
Let $T$ be a set of terms. Recall that the mapping $S : T \to T$ is defined so that $S(t)$ is the smallest set such that

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

Prove the following:

1. $S(A \cup B) = S(A) \cup S(B)$
2. $S$ is idempotent: $S(S(A)) = S(A)$

3. $S$ is monotonic: 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 8**

We define the notion of simple proof: A proof $P$ is simple if each node appears at most once in each branch of $P$.

Prove that if $P$ is a minimal proof of $T \vdash u$ then $P$ is a simple proof of $T \vdash u$.

**Exercise 9**

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 10**

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

**Exercise 11 (Final 2009-2010)**

We recall Dolev-Yao intruder deduction system:

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

Consider the following protocol

\[A \rightarrow S : \langle A \rangle_{K_S}, \langle B \rangle_{K_S}, \{A \oplus N_A\}_{K_S} >\]

\[A \rightarrow S : \langle N_A \oplus B \rangle_{K_S}, \{A \oplus c\}_{K_S} >\]

\[B \rightarrow S : \langle B \rangle_{K_S}, \{A\}_{K_S}, \{B \oplus N_B\}_{K_S} >\]

\[B \rightarrow S : \langle N_B \oplus A \rangle_{K_S}, \{N_B \oplus c\}_{K_S} >\]

\[S \rightarrow A : K \oplus \{N_A\}_{K_S}\]

\[S \rightarrow B : K \oplus \{N_B\}_{K_S}\]

Where $c$ is a weak shared secret between $A$ and $B$, $\oplus$ is the exclusive-or and $K$ is a new fresh symetric key between $A$ and $B$ which has been generated by $S$. 

1. Modify the protocol in order to model the following property

\[ \{x \oplus y\}_{K_s} = \{x\}_{K_s} \oplus \{y\}_{K_s} \]

2. Extend the Dolev-Yao deduction system by adding an extra rule called (XOR) which models the intruder’s ability to use the xor.

3. In the extended deduction system, prove or disprove that \( K \) is a secret for a passive Dolev-Yao intruder?

\[ R_1 \quad C \cup \{T \models u\} \rightsquigarrow C \quad \text{if } T \cup \{x \mid T' \models x \in C, T' \subset T\} \models u \]

\[ R_2 \quad C \cup \{T \models u\} \rightsquigarrow_{\sigma} C\sigma \cup \{T\sigma \models u\sigma\} \quad \sigma = \text{mgu}(t,u), t \in \text{st}(T), \]

\[ R_3 \quad C \cup \{T \models u\} \rightsquigarrow_{\sigma} C\sigma \cup \{T\sigma \models u\sigma\} \quad \sigma = \text{mgu}(t_1, t_2), t_1, t_2 \in \text{st}(T), \]

\[ R_4 \quad C \cup \{T \models \{u\}_v\} \rightsquigarrow C \cup \{T \models u, T \models v\} \]

\[ R_5 \quad C \cup \{T \models \langle u, v \rangle\} \rightsquigarrow C \cup \{T \models u, T \models v\} \]

\[ R_6 \quad C \cup \{T \models u\} \rightsquigarrow \bot \quad \text{if } T = \emptyset \text{ or } \text{var}(T) = \text{var}(u) = \emptyset \text{ and } T \not\models u \]

**Exercise 12**

Denning-Sacco Protocol

1. \( A \rightarrow S : \langle A, B \rangle \)

2. \( S \rightarrow A : \{\langle\langle B, N_{AB}\rangle, \langle N_s, \langle\langle N_{AB}, \langle A, N_s\rangle\rangle_{K_{BS}}\rangle\rangle_{K_{AS}}\}\} \]

3. \( A \rightarrow B : \{\langle N_{AB}, \langle A, N_s\rangle\rangle_{K_{BS}}\} \]

4. \( B \rightarrow A : \{s_{AB}\}_{N_{AB}} \]

Give a role specification of this protocol of an instance of execution between \( A, S \) and \( B \).

**Exercise 13**

\[ A \rightarrow B : \langle A, N_A \rangle \]

\[ B \rightarrow A : \{\langle N_A, N_B\rangle\}_{K_{ab}} \]

\[ A \rightarrow B : N_B \]

\[ B \rightarrow A : \{\langle K, N_B\rangle\}_{K_{ab}} \]

\[ A \rightarrow B : \{s\}_K \]

Intruder knows only identities of \( A \) and \( B \).

- Give role specification of this protocol of an instance of execution between \( A \) and \( B \).
- Give a constraint system associated to this protocol between \( A \) and \( B \).
Exercise 14

\[ A \to B : \langle A, N_A \rangle \]
\[ B \to A : \{\langle N_A, N_B \rangle \}_K^{ab} \]
\[ A \to B : N_B \]
\[ B \to A : \{\langle K, N_B \rangle \}_K^{ab} \]
\[ A \to B : \{s\}_K \]

Intruder knows only identities of A and B.

- There exists an easy attack, can you find it ?
- Give the associated interleaving for this attack and write the constraints system associated.
- Use simplification rules to transform the system in solved form.

Exercise 15

\[ A \to B : \{\langle A, K \rangle \}_K^{ab} \]
\[ B \to A : \{s\}_K^{ab} \]

Intruder knows only identities of A and B. Show that the secret data \(s\) is preserved by one single session between A and B.

Exercise 16 (Final 2007)

Active Intruder: Consider the following protocol:

\[ A \to B : \{\langle B, N_A \rangle \}^{pk(B)} \]
\[ B \to A : \{\langle N_A, \langle N_B, B \rangle \rangle \}^{pk(A)} \]
\[ A \to B : \{N_B\}^{pk(B)} \]

1. Prove there is no attack against the secret \(N_B\) in presence of a passive Intruder.
2. Give a modeling by roles of this protocol.
3. Find an attack against an active intruder on this protocol.
4. Correct the protocol to avoid this attack.

Exercise 17 (Final 2010)

We consider the following protocol called FFFGGG:

1 \[ A \to B : A \]
2 \[ B \to A : B, N, M, O \]
3 \[ A \to B : A, \{N, M, O, S\}^{pk_B} \]
4 \[ B \to A : N, X, \{X, Y, S, N\}^{pk_B} \]
We omit to write pairing, you can do the same in your solution. In step 3, if $B$ receives the message $A, \{N, X, Y, S\}_{pkB}$ then he only checks the correspondance of $N$ and sees the other data as variables.

- Give the role description of the protocol.
- Give an attack on this protocol showing that $S$ is not secret

**Exercise 18 (Final 2010)**

We recall the role description of Needham Schroeder protocol:

$$R_A = (\text{init}, X_b \rightarrow \{<N_a, A>\}_{pk(X_b)}),$$

$$\quad (\{<N_a, x_{N_b}>\}_{pk(A)} \rightarrow \{x_{N_b}\}_{pk(X_b)}),$$

$$R_B = (\{<x_{N_a}, x_A>\}_{pk(B)} \rightarrow \{<x_{N_a}, N_b>\}_{pk(x_A)}),$$

$$\quad (\{N_b\}_{pk(B)} \rightarrow stop)$$

1. Recall the attack found by Lowe called man in the middle
2. Propose an interleaving and construct the associated constraint system.
3. Solve the constraint system in order to recover from the attack.