Exercise 1
(8 points) Give the mgu between $t$ and $u$ for the following terms, where $x, y, z$ are variables and $a, b$ constants:

- $t = \langle a, \{z\}_b \rangle$ and $s = \langle x, y \rangle$
- $t = \langle \{x\}_b, \{y\}_b \rangle$ and $s = \langle \{a\}_b, z \rangle$
- $t = \langle \{z, a\}_x \rangle$ and $s = \langle \{y, \{x\}_b\} \rangle$
- $t = \langle \{a, z\}_x \rangle$ and $s = \langle \{y, \{x\}_b\} \rangle$

Exercise 2
(15 points) 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.

- $T_1 = \{\langle m_1, m_2 \rangle, \{m_1, m_4\}_m, m_4, m_5, m_6, \{m_4, m_7\}_m, m_7\}$ and $s = \{m_1\}_1$.
- $T_1 = \{\{a\}_k, \{c\}_a, \{k\}_1\}_a\}$ and $s = c$.
- $T_1 = \{\langle m_1, m_2 \rangle, \{m_1, m_4\}_m, m_4, m_5, m_6, \{m_4, m_7\}_m, m_7\}$ and $s = m_5$.
- $T_1 = \{\{k_1, k_2\}_k, m\} \{m\}_1\}$ and $s = k_2$.

Exercise 3
(20 points) Active Intruder: Consider the following protocol:

$$A \rightarrow B : \{B, \langle N_A \rangle_{pk(B)}\}$$
$$B \rightarrow A : \{\langle N_A, \langle N_B, B \rangle \rangle_{pk(A)}\}$$
$$A \rightarrow B : \{N_B\}_{pk(B)}$$

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 4
(12 points)

1. (8 pts) Assume the following scenario in a BLP model. The security labels are:
   - two security levels = \{high, low\}, where low < high, and
   - two categories = \{army, nuclear\}. 
The categories the following objects belong to and their security levels are:

<table>
<thead>
<tr>
<th>Object</th>
<th>Category</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>army location</td>
<td>army</td>
<td>low</td>
</tr>
<tr>
<td>nuclear code</td>
<td>nuclear</td>
<td>high</td>
</tr>
<tr>
<td>number of army units</td>
<td>army</td>
<td>low</td>
</tr>
<tr>
<td>number of nuclear units</td>
<td>nuclear</td>
<td>high</td>
</tr>
</tbody>
</table>

The clearances for Alice and Bob are:

<table>
<thead>
<tr>
<th>Name</th>
<th>Category</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>army, nuclear</td>
<td>high</td>
</tr>
<tr>
<td>Bob</td>
<td>nuclear</td>
<td>low</td>
</tr>
</tbody>
</table>

Answer the following questions with respect to that lattice and explain your answer:

(a) Can Alice change the army location?
(b) Can Alice calculate the sum of army and nuclear units?
(c) Can Bob change the army location?
(d) Assume the nuclear code has not been changed for the last 50 years. Can Bob increase this code by his favorite number?

Exercise 5

(30 points) Let $E : \{0, 1\}^k \times \{0, 1\}^l \rightarrow \{0, 1\}^l$ be a secure block cipher. Let $K$ be the key-generation algorithm that returns a random $k$-bit string as the key $K$. Let $E$ be the following encryption algorithm:

Algorithm $E_K(M)$
If $|M|$ is not a positive multiple of $l$ then return FALSE
Divide $M$ into $l$ bit blocks, $M = M[1] \ldots M[n]$
$P[0] \leftarrow R\{0, 1\}^l$; $C[0] \leftarrow E_K(P[0])$ For $i = 1, \ldots, n$ do
$P[i] \leftarrow P[i-1] \oplus M[i]$;
$C[i] \leftarrow E_K(P[i])$;
EndFor
$C \leftarrow C[0]C[1] \ldots C[n]$;
Return $C$

1. 10 points: Specify a decryption algorithm $D$ such that $SE = (K; E; D)$ is a symmetric encryption scheme with correct decryption. We are denoting the inverse of $E_K$ by $E_K^{-1}$

2. 20 points: Show that this scheme is insecure by presenting a practical adversary IND-CPA. Say what is the advantage achieved by your adversary.