Exercise 1
(15 points) Given the security levels TOP SECRET, SECRET, CONFIDENTIAL and UNCLASSIFIED (ordered from highest to lowest) and two categories: Nuclear and Army. We consider four subjects:

- the president has a TOP SECRET clearance for Nuclear and Army,
- the colonel has SECRET clearance for Army and Nuclear,
- the major has only CONFIDENTIAL clearance for Army, and
- the soldier has only UNCLASSIFIED clearance for Nuclear.

We also have some objects (documents):

- the army position at security level SECRET,
- the number of army units at security level CONFIDENTIAL,
- the number of nuclear units at security level CONFIDENTIAL,
- the costs of the nuclear program at security level UNCLASSIFIED,
- the costs of the army at security level UNCLASSIFIED, and
- the nuclear code at security level TOP SECRET.

1. (3 points) Recall Bell-LaPadula and Biba security models and explain the difference between the two models.

2. (1 points) Draw the lattice associated with this scenario.

3. (5 points) Place on the lattice all the objects and subjects.
4. (6 points) Answer with justifications the following questions based on the Bell-LaPadula model:

(a) Can the president compute the overall defense costs (army + nuclear)?
(b) Can the major compute the total number of nuclear and army units?
(c) Can the colonel compute the total number of nuclear and army units?
(d) Can the colonel change the army position?
(e) Can the major change the nuclear code?
(f) Can the soldier change the nuclear code?

Solution :

1. Here is the lattice of classifications:

2. Yes, the president can compute the total cost, since he has clearance \((T, \{A, N\})\), which dominates both the army cost, classified as \((U, \{A\})\), and the nuclear cost, classified as \((U, \{N\})\).

3. No, the major has no access to the number of nuclear units, since his compartment does not include Nuclear: he has clearance \((C, \{A\})\), which does dominate the number of army units, classified as \((C, \{A\})\), but not the number of nuclear units, classified as \((C, \{N\})\).

4. Yes, the colonel can read these numbers, since read-below is allowed and he has clearance \((S, \{A, N\})\), which dominates both the number of army units, classified as \((C, \{A\})\), and the number of nuclear units, classified as \((C, \{N\})\).

5. No, because write-down is forbidden and the colonel has clearance \((T(S, \{A, N\})\), which dominates the army position, classified as \((S, \{A\})\). Otherwise, the colonel could leak some nuclear informations into the army Location document.

NOTICE: An extension of the basic model provides a mechanism for allowing trusted subjects to break the rules in a controlled way to allow this type of communication. Trusted subjects have a maximum security level and a current security level. The maximum security level must dominate the current security level. A trusted subject may (effectively) decrease its security level from the maximum in order to communicate with entities at lower security levels. In our example, we can use this mechanism to allow the colonel to downgrade his current security level to \(T(S, \{A\})\) and change the army position.

6. No, there is no relation between the clearance of the major \((C, \{A\})\) and the nuclear code classified as \((T, \{N\})\).

7. Yes, write-up is possible: the soldier has clearance \((U, \{N\})\) and the nuclear code is classified as \((T, \{N\})\).
8. Question 4f shows that the integrity of data is not preserved in this model.

**Exercise 2**
(10 points) Consider the following control access in a bank, where users are Alice, Bob, Charlie and John:

<table>
<thead>
<tr>
<th>User</th>
<th>Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>read account of Mr X</td>
</tr>
<tr>
<td>Alice</td>
<td>read account of Mr Y</td>
</tr>
<tr>
<td>Alice</td>
<td>write in project New Bank</td>
</tr>
<tr>
<td>Alice</td>
<td>start application Money</td>
</tr>
<tr>
<td>Alice</td>
<td>start application Create New client</td>
</tr>
<tr>
<td>Bob</td>
<td>read account of Mr Y</td>
</tr>
<tr>
<td>Bob</td>
<td>write in project New Bank</td>
</tr>
<tr>
<td>Bob</td>
<td>start application Create New client</td>
</tr>
<tr>
<td>Bob</td>
<td>read account of Mr X</td>
</tr>
<tr>
<td>Charlie</td>
<td>read account of Mr X</td>
</tr>
<tr>
<td>Charlie</td>
<td>read account of Mr Y</td>
</tr>
<tr>
<td>Charlie</td>
<td>write in project New Bank</td>
</tr>
<tr>
<td>Charlie</td>
<td>start application Create New client</td>
</tr>
<tr>
<td>John</td>
<td>read account of Mr Y</td>
</tr>
<tr>
<td>John</td>
<td>start application Money</td>
</tr>
<tr>
<td>John</td>
<td>start application Create New client</td>
</tr>
</tbody>
</table>

Propose a RBAC model for improving this situation.

**Solution:**
*User are:* Alice, Bob, Charlie and John
*Admin are:* Alice, Bob and Charlie
*Superuser are:* Alice and John

<table>
<thead>
<tr>
<th>Role</th>
<th>Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>read account of Mr Y</td>
</tr>
<tr>
<td>User</td>
<td>start application Create New client</td>
</tr>
<tr>
<td>Admin</td>
<td>write in project New Bank</td>
</tr>
<tr>
<td>Admin</td>
<td>read account of Mr X</td>
</tr>
<tr>
<td>Superuser</td>
<td>start application Money</td>
</tr>
</tbody>
</table>

**Exercise 3**
(10 points) Let $\mathcal{E}$ be an IND-CCA2 secure encryption scheme. We modify this scheme into $\mathcal{E}'(m) = \mathcal{E}(m) || h(m)$, where $h$ is an hash function. This should help the user to detect some errors in the transmission of the messages. Prove that the new scheme $\mathcal{E}'$ is not IND-CPA. It means give an attack against IND-CPA for $\mathcal{E}'$. 
Solution:

- Consider the following adversary:

  Notice that $E'(m_b) = E||h(m_b)$
  
  $A_1(n, pk) : m_1, m_0, s$
  
  $A_2(n, pk, s, m_1, m_0, E'(m_b)) :$ if $h(m_0) = h(m_b)$ then return 0 else 1

Exercise 4 (10 points)

We recall Dolev-Yao intruder deduction system:

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

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

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

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

1. (3 points) Modify the protocol in order to model the following property

$$\{x \oplus y\}_{K_s} = \{x\}_{K_s} \oplus \{y\}_{K_s}$$

Where $A \rightarrow S : << \{A\}_{K_s}, \{B\}_{K_s}, \{A \oplus N_A\}_{K_s} >$

$A \rightarrow S : << \{N_A \oplus B\}_{K_s}, \{N_A \oplus c\}_{K_s} >$

$B \rightarrow S : << \{B\}_{K_s}, \{A\}_{K_s}, \{B \oplus N_B\}_{K_s} >$

$B \rightarrow S : << \{N_B \oplus A\}_{K_s}, \{N_B \oplus c\}_{K_s} >$

$S \rightarrow A : K \oplus \{N_A\}_{K_s}$

$S \rightarrow B : K \oplus \{N_B\}_{K_s}$
2. (2 points) We need to add the xor rule

\[
\begin{align*}
\text{(XOR) } & \quad \frac{T_0 \vdash u}{T_0 \vdash u \oplus v} \\
& \quad \frac{T_0 \vdash v}{T_0 \vdash u \oplus v}
\end{align*}
\]

3. (5 points) In the extended deduction system, prove or disprove that \( K \) is a secret for a passive Dolev-Yao intruder?

There are several proofs for deducing \( K \) from a normal execution of the protocol. For instance by using the first message send by \( B \), it is possible to deduce \( \{N_B\}^{K_s} \) by xoring the first part of the first pair \( \{B\}^{K_s} \) with \( \{B\}^{K_s} \oplus \{N_B\}^{K_s} \). Using this message for doing a xor with the last exchanged message we obtain \( K \). (A proof tree can be drawn)

**Solution**:

1. (3 points) Modify the protocol in order to model the following property

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

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

3. (5 points) In the extended deduction system, prove or disprove that \( K \) is a secret for a passive Dolev-Yao intruder?

**Exercise 5**

(20 points) We recall the Yahalom protocol, where \( K_{as}, K_{bs} \) and \( K_{ab} \) are symetric keys.

1. \( A \rightarrow B: \ A, N_A \)
2. \( B \rightarrow S: \ B, \{A, N_A, N_B\}^{K_{bs}} \)
3. \( S \rightarrow A: \ \{B, K_{ab}, N_A, N_B\}^{K_{as}}, \{A, K_{ab}\}^{K_{bs}} \)
4. \( A \rightarrow B: \ \{A, K_{ab}\}^{K_{bs}}, \{N_B\}^{K_{ab}} \)

1. (5 points) Give a role description of this protocol.
2. (5 points) Give a constraint system associated to your role description.
3. (10 points) Propose a type flaw attack on this protocol.

Hint: message 3 is not used in the attack.

**Solution**:

1. \( I(A) \rightarrow B: \ (A, N_A) \)
2. \( B \rightarrow I(S): \ (B, (A, N_A, N_B)^{K_{bs}}) \)
3. \( I(A) \rightarrow B: \ ((A, N_A, N_B)^{K_{bs}}, (N_B)_{N_A, N_B}) \)
Exercise 6
(15 points) Zheng & Seberry in 1993 proposed the following encryption scheme:

\[ f(r) || (G(r) \oplus (x||H(x))) \]

where \( x \) is the plain text, \( f \) is a one way trap-door function (like RSA), \( G \) and \( H \) are two public hash functions, || denotes the concatenation of bitstrings and \( \oplus \) is the exclusive-or operator.

- (5 points) Give the associated decryption algorithm.

- (10 points) Give an IND-CCA2 attack against this scheme.
  Hint: you cannot ask the cipher of \( m_b \) to the decryption oracle, but a cipher of \( m_{\overline{b}} \) is not forbidden...

Solution:

- Give the associated decryption algorithm.
  First decrypt \( f(r) \) to get \( r \), then compute \( G(r) \) and xor the result with \( G(r) \oplus (x||H(x)) \) to get \( x||H(x) \) then check if the application of \( H \) on the first element of the concatenation is equal to the second to be sure that you get the right plaintext.

- Give an IND-CCA2 attack against this scheme.
  Hint: you cannot ask the cipher of \( m_b \) to the decryption oracle, but a cipher of \( m_{\overline{b}} \) is not forbidden...
  First part of the adversary chooses \( m_1 \) and \( m_0 \)
  \( c = f(r) || (G(r) \oplus (m_b||H(m_b))) \)
  the second adversary computes \( m_0||H(m_0) \) and \( m_1||H(m_1) \)
  And give to the decryption oracle
  \( c' = f(r) || (G(r) \oplus (m_b||H(m_b))) \oplus (m_0||H(m_0)) \oplus (m_1||H(m_1)) \)
  Indeed \( c' = f(r) || (G(r) \oplus (m_{\overline{b}}||H(m_{\overline{b}}))) \)
  Hence the decryption oracle answers \( m_{\overline{b}} \) then if \( m_{\overline{b}} = m_0 \) then he outputs 1 else 0.