Problem 1 (30 points)

Shown below is the initiation part of the Public Key Kerberos protocol in which the client obtains a “ticket granting ticket” (TGT) from the Kerberos Authentication Server (KAS), and also a key AK that the client uses later to communicate with the Ticket Granting Server (TGS). AK is also contained in TGT, and the TGT is encrypted with a long-term key shared between KAS and TGT.

\[
\begin{align*}
C \rightarrow K & : \text{Cert}_C, SIG_C\{t_C, n_1\}, C, T, n_2 \\
K \rightarrow C & : \text{ENC}_{pk_C}\{\text{Cert}_K, SIG_K\{k, n_1\}\}, C, \text{ENC}_{k_{KT}}\{\text{TGT}\}, \text{ENC}_k\{AK, n_2, t_K, T\}
\end{align*}
\]

Figure 1: The AS exchange protocol in Public Key Kerberos

Here C is the client and K is the KAS. We abbreviate by \(SIG_C\{m\}\) the message \(m\), \(SIG_C\{m\}\). \(n_1, n_2\) are nonces, \(t_C, t_K\) are timestamps, \(T\) is the name of the TGS. \(\text{Cert}_C, \text{Cert}_K\) are certificates of the client and KAS respectively. \(pk_C\) is the public key of the Client, \(k\) is a fresh key generated by KAS and \(k_{KT}\) is a long-term key shared between KAS and TGT.

Part a (10 points)

State informally the authentication requirement for the above protocol.

Part b (10 points)

In 3-4 sentences argue informally whether the authentication requirement from Part a is satisfied by the protocol. If the protocol does not satisfy this requirement, demonstrate an attack and suggest a fix.
Part c (10 points)

Briefly explain the security guarantee you get if the Murphi model checker finds no errors in this protocol. Clearly list the simplifications made in constructing the model and how these assumptions can fail in the presence of a more powerful adversary.

Problem 2 (30 points)

The $Q_{DL}$ protocol shown below hides the nonce generated by the initiator. The initiator’s and responder’s program are given below:

$\text{Init}_{DL} \equiv [\text{new } x; gx := \expg x]X(gx) \quad \text{Resp}_{DL} \equiv []X$

We can prove the following for this protocol

$\Gamma_1 \vdash \text{Start}(X)[\text{Init}_{DL}]X\text{Fresh}(X,gx)$

where $\Gamma_1$ is empty.

The one-way authentication protocol $Q_{CR}$ is shown below. The initiator does not generate the nonce but it is provided as a parameter to the initiator. The authentication property of the protocol depends on the nonce parameter being fresh. The initiator’s and responder’s program are given below:

$\text{Init}_{CR} \equiv (\hat{Y},m_1)[
\quad \text{send } \hat{X},\hat{Y},m_1;
\quad \text{receive } \hat{Y},\hat{X},s;
\quad \text{verify } s,(m_1,\hat{X}),\hat{Y};
\quad ]X()$

$\text{Resp}_{CR} \equiv ()[
\quad \text{receive } \hat{X},\hat{Y},x;
\quad r := \text{sign}(x,\hat{X}),\hat{Y};
\quad \text{send } \hat{Y},\hat{X},r;
\quad ]Y()$

We can prove the following for this protocol

$\Gamma_2 \vdash_{Q_{CR}} \text{Fresh}(X,m_1)[\text{Init}_{CR}]X\text{Honest}(\hat{Y}) \land \hat{Y} \neq \hat{X} \supset \phi_{auth}$.

$\phi_{auth} \equiv \exists Y. (\text{Receive}(Y,(\hat{X},\hat{Y},m_1)) < \text{Send}(Y,(\hat{Y},\hat{X},SIG_Y\{m_1,\hat{X}\}))$)

A modified version of the invariant used in proving the above is given below. You can use this invariant in Part c of this problem.

$\Gamma_2 \equiv \text{Honest}(\hat{Y}) \supset \forall \hat{X},t,m. (\text{Send}(Y,t) \land \text{Contains}(t,SIG_Y\{m,\hat{X}\}) \supset 
(\text{Receive}(Y,(\hat{X},\hat{Y},m)) < \text{Send}(Y,(\hat{Y},\hat{X},SIG_Y\{m,\hat{X}\}))$)
A sequential composition $Q_{COM}$ of the protocols is shown below

$$
\begin{align*}
\text{Init}_{COM} & \equiv (\hat{Y})[
\text{new } m_1; \\
& \quad gm_1 := \text{exp} g m_1; \\
& \quad \text{send } \hat{X}, \hat{Y}, gm_1; \\
& \quad \text{receive } \hat{Y}, \hat{X}, s; \\
& \quad \text{verify } s, (gm_1, \hat{X}), \hat{Y}; \\
]x() \\
\text{Resp}_{COM} & \equiv ()[
\text{receive } \hat{X}, \hat{Y}, x; \\
& \quad r := \text{sign} (x, \hat{X}), \hat{Y}; \\
& \quad \text{send } \hat{Y}, \hat{X}, r;
]Y()
\end{align*}
$$

Part a (5 points)
State in the syntax of PCL the authentication property of $Q_{COM}$.

Part b (10 points)
Argue informally how the properties of $Q_{DL}$ and $Q_{CR}$ can be combined to derive the property of $Q_{COM}$ from Part a.

Part c (15 points)
Now provide a formal proof of the property from Part a that follows the structure of the informal argument in Part b using the sequential composition theorem of PCL.

Problem 3 (40 points)

Part a (5 × 3 = 15 points)
In this problem, we consider an active network adversary who can perform arbitrary probabilistic polynomial time (PPT) computation. Consider the following three scenarios. For each scenario, state the weakest notion of security (among IND-CPA and IND-CCA) that the encryption scheme needs to satisfy in order to guarantee secrecy of the specified payload in the presence of the adversary. Briefly justify the choice of the security notion.

1. Using SSL, honest parties $A$ and $B$ have already established a shared key $k$. $A$ sends message $m$ to $B$ encrypted with $k$. $B$ decrypts the ciphertext, re-encrypts it with $k$ and sends it back to $A$. The payload is the message $m$ and the adversary is an active network adversary.

2. A spaceship $S$ sends data encrypted with the public key of a space station $SS$ to $SS$ that then relays this data to earth using a long term shared key $k$. An alien $A$ from Mars has learnt $k$. $A$ tries to fool $S$ into sending the message “Do not attack Mars” to $SS$, but is not sure at this point if it succeeded, i.e. $A$ is not sure if the message $m$ sent by $S$ to $SS$ is “Do
not attack Mars” or some other text. SS realizes that \( k \) has been compromised and so it forwards the message \( m \) to earth with an alternate shared key \( k' \) that is not known to \( A \). The payload is the message \( m \) and the adversary is the alien \( A \).

3. Nations \( X \) and \( Y \) are at war, and they have warships \( WX \) and \( WY \) out at sea. \( WX \) knows that any message it sends to its base station in the clear will be intercepted by \( WY \), then encrypted with a shared key \( k_Y \) and sent to \( WY \)’s base station. \( WY \) sends a message \( m \) encrypted with key \( k_Y \) where \( m \) is not sent by \( WX \) that was intercepted by \( WY \). The payload is the message \( m \) and the adversary is \( WX \).

**Part b (5 \times 5 = 25 \text{ points})**

This problem requires you to walk through the proof of the computational soundness theorem of the Abadi-Rogaway logic of encrypted expressions, which was discussed in class. Consider the following two expressions \( M \) and \( N \). Assume that \( \Pi \) is a type-0 secure encryption scheme. We want to show that \( [M]_\Pi \approx [N]_\Pi \).

\[
M = \{K_3\} K_1 \{K_2\} K_1 \{11\} K_2 \{K_5\} K_4 \{00\} K_2 \{101\} K_5
\]
\[
N = \{K_3\} K_1 \{K_2, 00\} K_3 \{K_5\} K_4 \{K_6, K_6\} K_2 \{101\} K_5
\]

1. Write down the patterns for \( M \) and \( N \) and verify that they are equal.

2. Renumber the keys in \( M \) and \( N \) so that “deeper” keys have lower numbers to get the expressions \( M' \) and \( N' \). Explain why \( \text{pattern}(M') = \text{pattern}(N') \). State a syntactic restriction on expressions that is essential for this renumbering to be possible.

3. Write down the hybrids \( M_j \) and \( N_k \) where \( 0 \leq j \leq m \) and \( 0 \leq k \leq n \), such that \( M_m = M' \), \( N_n = N' \) and \( M_0 = N_0 = \text{pattern}(M') = \text{pattern}(N') \).

4. To do the reduction proof, assume that \( [M']_\Pi \approx [N']_\Pi \) does not hold. Thus, there exists a PPT adversary that can distinguish between \( [M']_\Pi \) and \( [N']_\Pi \) with non-negligible probability. Explain why this implies that there exists an adversary that has a non-negligible probability of distinguishing between ensembles of at least one pair of adjacent hybrids from the previous step.

5. Explain how an attacker that has a non-negligible probability of distinguishing between ensembles of adjacent hybrids can be used to construct another attacker that breaks the type-0 security of \( \Pi \).