MTAT.07.003 Cryptology II
Spring 2012 / Exercise session ?? / Example Solution

Exercise (Alternative definitions for IND-CPA security). *Estimate computational distance between following games under the assumption that* $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *is* (t, ε)*-IND-CPA secure cryptosystem.*

1. *Left-or-right games (LOR security games)*

```
$\mathcal{G}_0^{\mathcal{A}}$
    $\mathsf{sk} \leftarrow \mathsf{Gen}$
    For $i = 1, \ldots, q$ do
        $(m_0^i, m_1^i) \leftarrow \mathcal{A}$
        Give $\mathsf{Enc}_{\mathsf{sk}}(m_0^i)$ to $\mathcal{A}$
    return the output of $\mathcal{A}$

$\mathcal{G}_1^{\mathcal{A}}$
    $\mathsf{sk} \leftarrow \mathsf{Gen}$
    For $i = 1, \ldots, q$ do
        $(m_0^i, m_1^i) \leftarrow \mathcal{A}$
        Give $\mathsf{Enc}_{\mathsf{sk}}(m_1^i)$ to $\mathcal{A}$
    return the output of $\mathcal{A}$
```

2. *Real-or-random games (ROR security games)*

```
$\mathcal{G}_0^{\mathcal{A}}$
    $\mathsf{sk} \leftarrow \mathsf{Gen}$
    For $i = 1, \ldots, q$ do
        $m^i \leftarrow \mathcal{A}$
        Give $\mathsf{Enc}_{\mathsf{sk}}(m^i)$ to $\mathcal{A}$
    return the output of $\mathcal{A}$

$\mathcal{G}_1^{\mathcal{A}}$
    $\mathsf{sk} \leftarrow \mathsf{Gen}$
    For $i = 1, \ldots, q$ do
        $m_0^i \leftarrow \mathcal{A}, m_1^i \xleftarrow{u} \mathcal{M}$
        Give $\mathsf{Enc}_{\mathsf{sk}}(m_1^i)$ to $\mathcal{A}$
    return the output of $\mathcal{A}$
```

Moreover, we can suse these security games to define (t, ε)*-LOR security and* (t, ε)*-ROR security. Prove that security against these security notions also implies IND-CPA security.*

Solution. We split the proof into separate blocks each dedicates to a single subgoal.

Subproof IND-CPA⇒ LOR-SECURITY

Subproof LOR-SECURITY⇒IND-CPA

Subproof IND-CPA⇒ LOR-SECURITY

Subproof ROR-SECURITY⇒IND-CPA