Lemma: \( CBC^E \) and \( CBC^P \) are indistinguishable.

Proof:

So, \( CBC^E \) and \( CBC^P \) as \( E \) and \( P \) are distinct.

By some argument as before, \( CBC^E \) and \( CBC^P \) are indistinguishable.

Lemma: \( CBC^E \) and \( CBC^P \) are indistinguishable if \( E \) is a \((+q, E)\) PRP.

Proof: Suppose \( A \) can distinguish \( CBC^E \) and \( CBC^P \). Then, \( B^E = A^{cbc^E} \) can distinguish \( E \) and \( P \), running time of \( B^E \) is \( t \) running time of \( A + cbc \) operations.

Then: \( CBC^E \) is \((+q, E)\) \(R\)-or-\(R\) secure if \( E \) is \((+q, E)\) \(R\)-or-\(R\) secure.

Proof: \( CBC^E \) is \((+q, E)\) \(R\)-or-\(R\) secure if \( E \) is \((+q, E)\) \(R\)-or-\(R\) secure.

Alternative Definitions of Security:

Def.: \( T_i(x_i) = x_i \)

Def.: (Left Right (LR) security) \( E \) is \((+q, E)\) LR secure if

\[ \text{Ex o T}_0 \rightarrow \text{Ex o T}_1 \]

Thm: \( E \) is \((+q, E)\) \(R\)-or-\(R\) secure iff \( E \) is \((+q, E)\) LR secure.

Queries must be for pairs of equal length.
Proof: \( LR \Rightarrow R-or-R \) (by contrapositive)

Suppose \( A \) can \((+q, E)\) \( R-or-R \) break \( E \).

Then let \( B E \to \nu_i = A E \to \nu_i \circ (\cdot, g(\cdot)) \).

\[
\begin{array}{c}
\text{B} \\
\downarrow \\
\text{A} \\
\end{array}
\begin{array}{c}
\rightarrow \nu_i \\
\rightarrow E \\
\end{array}
\]

\( E \to \nu_i \circ (\cdot, g(\cdot)) = E \) \quad \( E \to \nu_i = E \cdot g \)

So, \( B \) can \((+O(g), q, E)\) \( LR \) break \( E \).

\( R-or-R \Rightarrow LR \) (direct proof)

\[ (\text{type} E) R-or-R \Rightarrow E \xrightarrow{g} E \cdot \nu_i \]

\[ E \to \nu_i \circ g = E \cdot \nu_i \circ \nu_i \] \quad \text{if } |m_a| = |m_i|

and \( E \to \nu_i \circ \nu_i \)

If \( A \) distinguishes \( E \to \nu_i \) and \( E \to \nu_i \circ \nu_i \)

\[
\begin{array}{c}
\text{B} \\
\downarrow \\
\text{A} \\
\end{array}
\begin{array}{c}
\rightarrow \nu_i \\
\rightarrow E \\
\end{array}
\]

A is good at telling \( E \) and \( E \cdot \nu_i \) apart.

\[ E \cdot \nu_i \circ \nu_i = E \cdot \nu_i \circ \nu_i \] \quad \text{if } |m_a| = |m_i|

By transitivity, \( E \to \nu_i \xrightarrow{g} E \cdot \nu_i \).
Semantic Security

Oracle $E_K \circ S_b$

$S_b(M)$

$m \leftarrow M$

$m' \leftarrow M$

(return $T_b(m, m')$)

$Adv_A = \left| Pr[A^{E_K S_b} = (f, f(m, m_2, \ldots, m_g))] - Pr[A^{E_K S_b} = (f, f(m, m_2, \ldots, m_g))] \right|$

given ciphertext & messages

given garbage

Then Semantic Security is equivalent to LR security

Proof Semantic $\Rightarrow$ LR (by contrapositive)

turn each single query into two