1. First, we fix a message $m_0$.

For any $sk, r \in \{0, 1\}^n$, define the following set:

$$C_{sk,r} = \{ m \mid \exists sk' \in \{0, 1\}^n, D_{sk'}(E_{sk}(m_0, r)) = m \}.$$

Notice that if we choose $m_1 \leftarrow \{0, 1\}^\ell$ uniformly then the probability that $m_1 \in C_{sk,r}$ is at most $2^n/2^\ell \leq 2^{-10}$ since the size of $C_{sk,r}$ is limited by $2^n$ because there are $2^n$ keys and there can only be one decryption of a specific ciphertext per key (otherwise decryption would be impossible) thus there are at most $2^n$ decryptions of $E_{sk}(m_0, r)$, and because $m_1$ was chosen uniformly.

In particular the above holds for random $sk, r$. Formally, because:

$$\Pr_{sk,r,m_1}[m_1 \in C_{sk,r}] = E_{sk,r}[\Pr_{m_1}[m_1 \in C_{sk,r}]] \leq 2^{-10}.$$

Now we can fix such specific $m_1$. Formally, because:

$$\Pr_{sk,r,m_1}[m_1 \in C_{sk,r}] = \Pr_{m_1}[\Pr_{sk,r}[m_1 \in C_{sk,r}]] \leq 2^{-10}.$$

Therefore, there exists some $m_1 \in \{0, 1\}^\ell$ s.t. $\Pr_{sk,r}[m_1 \in C_{sk,r}] \leq 2^{-10}$, otherwise the expectation above would have to be greater than $2^{-10}$. This will be the $m_1$ that will be referred to in the rest of the proof.

The algorithm $A$ will do the following:

given a ciphertext $ct$:

- Go over all possible keys: $sk' \in \{0, 1\}^n$. if there exists some key s.t. $D_{sk'}(ct) = m_1$, return $m_1$.
- Otherwise, return $m_0$.

Notice that by the definition of $A$:

$$\Pr_{sk,r,m_1}[A(ct) = m_1 \mid b = 1] = \Pr_{sk,r}[\exists sk' \in \{0, 1\}^n \text{ s.t. } m_1 = D_{sk'}(ct) \mid ct \leftarrow E_{sk}(m_1, r)] = 1.$$

Since if $b = 1$ then for $sk, r$ that were chosen: $ct = E_{sk}(m_1, r)$ and then for $sk$: $D_{sk}(ct) = m_1$, thus $A$ returns $m_1$ as desired. Also by the definition of $m_1$,

$$\Pr_{sk,r}[A(ct) = m_1 \mid b = 0] = \Pr_{sk,r}[m_1 \in C_{sk,r}] \leq 2^{-10} \Rightarrow \Pr_{sk,r}[A(ct) = m_0 \mid b = 0] \geq 1 - 2^{-10}.$$

Therefore by law of total probability:

$$\Pr[A(ct) = m_b] = \Pr[b = 0] \Pr[A(ct) = m_0 \mid b = 0] + \Pr[b = 1] \Pr[A(ct) = m_1 \mid b = 1] \geq \frac{1}{2}(1+1-2^{-10}) > 0.99.$$

\[\square\]

1 Notice that the definition of this set is dependent on $sk, r$ and may be different for each pair of $sk, r$

2 This implies of course that $m_1 \neq m_0$, otherwise the statement would not be correct
2. Collaborators: Ben Liderman, Shany Ben-David.

(a) First, notice that by law of total probability:

\[
\Pr[A(x) = b \mid b \in \{0, 1\}, x \in X_b] = \\
\Pr[b = 0] \Pr[A(x) = 0 \mid b = 0, x \in X_0] + \Pr[b = 1] \Pr[A(x) = 1 \mid b = 1, x \in X_1] = \\
\frac{1}{2} (\Pr[A(X_0) = 0] + \Pr[A(X_1) = 1]) = \frac{1}{2} (1 - \Pr[A(X_0) = 1] + \Pr[A(X_1) = 1]) = \\
\frac{1}{2} + \frac{1}{2} (\Pr[A(X_1) = 1] - \Pr[A(X_0) = 1])
\]

Therefore, by definition:

\[
\left| \Pr[A(x) = b \mid b \in \{0, 1\}, x \in X_b] - \frac{1}{2} \right| = \frac{1}{2} \Pr[A(X_1) = 1] - \Pr[A(X_0) = 1] = \frac{\Delta_A(X_0, X_1)}{2}.
\]

\(\square\)

(b) We will prove the following two statements:

i. \(\max_A \Delta_A(X_0, X_1) = \max_{T \subseteq S} [\Pr[X_0 \in T] - \Pr[X_1 \in T]]\)

ii. \(\frac{1}{2} \sum_{x \in S} [\Pr[X_0 = x] - \Pr[X_1 = x]] = \max_{T \subseteq S} [\Pr[X_0 \in T] - \Pr[X_1 \in T]]\)

Proof of (i):

We will show that:

\[
\max_A \Delta_A(X_0, X_1) \leq \max_{T \subseteq S} [\Pr[X_0 \in T] - \Pr[X_1 \in T]]
\]

And also:

\[
\max_A \Delta_A(X_0, X_1) \geq \max_{T \subseteq S} [\Pr[X_0 \in T] - \Pr[X_1 \in T]]
\]

This will conclude our proof.

First, we’ll show:

\[
\max_A \Delta_A(X_0, X_1) \leq \max_{T \subseteq S} [\Pr[X_0 \in T] - \Pr[X_1 \in T]].
\]

Consider some function \(A : S \rightarrow \{0, 1\}\), and define \(T = \{x \in S \mid A(x) = 1\}\), we get that by definition:

\[
\Delta_A(X_0, X_1) = |\Pr[A(X_0 = 1)] - \Pr[A(X_1 = 1)]| = |\Pr[X_0 \in T] - \Pr[X_1 \in T]|.
\]

Specifically for a function \(A\) that achieves the maximal value of \(\Delta_A(X_0, X_1)\), there exists \(T \subseteq S\) for which:

\[
\Delta_A(X_0, X_1) = |\Pr[A(X_0 = 1)] - \Pr[A(X_1 = 1)]| = |\Pr[X_0 \in T] - \Pr[X_1 \in T]|.
\]

By the above claim, therefore:

\[
\max_A \Delta_A(X_0, X_1) \leq \max_{T \subseteq S} |\Pr[X_0 \in T] - \Pr[X_1 \in T]|.
\]

Similarly, for any \(T \subseteq S\), there exists a function \(A(x) = \begin{cases} 
1, & x \in T \\
0, & \text{o.w.}
\end{cases}\) such that:

\[
\Delta_A(X_0, X_1) = |\Pr[A(X_0 = 1)] - \Pr[A(X_1 = 1)]| = |\Pr[X_0 \in T] - \Pr[X_1 \in T]|.
\]
Which also leads to the conclusion that for a \( T \subseteq S \) that achieves maximal value of \( |\Pr [X_0 \in T] - \Pr [X_1 \in T]| \) there exists a function \( A \) for which:

\[
\Delta_A(X_0, X_1) = |\Pr [X_0 \in T] - \Pr [X_1 \in T]|
\]

Thus:

\[
\max_A \Delta_A(X_0, X_1) \geq \max_{T \subseteq S} |\Pr [X_0 \in T] - \Pr [X_1 \in T]|
\]

Proof of (ii):

First, we will show that: \( \forall T \subseteq S : \frac{1}{2} \sum_{x \in S} |\Pr [X_0 = x] - \Pr [X_1 = x]| \geq |\Pr [X_0 \in T] - \Pr [X_1 \in T]| \), then we’ll show that there exists \( T \subseteq S \) such that:

\[
\frac{1}{2} \sum_{x \in S} |\Pr [X_0 = x] - \Pr [X_1 = x]| = |\Pr [X_0 \in T] - \Pr [X_1 \in T]| ,
\]

and this will conclude the proof.

For any \( T \subseteq S \):

\[
\frac{1}{2} \sum_{x \in S} |\Pr [X_0 = x] - \Pr [X_1 = x]| = \frac{1}{2} \left( \sum_{x \in T} |\Pr [X_0 = x] - \Pr [X_1 = x]| + \sum_{x \in S \setminus T} |\Pr [X_0 = x] - \Pr [X_1 = x]| \right)
\]

\[
\geq \frac{1}{2} \left( \sum_{x \in T} |\Pr [X_0 = x] - \Pr [X_1 = x]| + \sum_{x \in S \setminus T} |\Pr [X_0 = x] - \Pr [X_1 = x]| \right)
\]

\[
= \frac{1}{2} (|\Pr [X_0 \in T] - \Pr [X_1 \in T]| + |\Pr [X_0 \notin T] - \Pr [X_1 \notin T]|)
\]

\[
= \frac{1}{2} (|\Pr [X_0 \in T] - \Pr [X_1 \in T]| + |1 - \Pr [X_0 \in T] - 1 + \Pr [X_1 \in T]|)
\]

\[
= \frac{1}{2} \cdot 2|\Pr [X_0 \in T] - \Pr [X_1 \in T]| = |\Pr [X_0 \in T] - \Pr [X_1 \in T]| ,
\]

Overall we have shown that: \( \forall T \subseteq S : \frac{1}{2} \sum_{x \in S} |\Pr [X_0 = x] - \Pr [X_1 = x]| \geq |\Pr [X_0 \in T] - \Pr [X_1 \in T]| , \)

as desired.

Now, we only need to show that there exists \( T \subseteq S \) such that:

\[
\frac{1}{2} \sum_{x \in S} |\Pr [X_0 = x] - \Pr [X_1 = x]| = |\Pr [X_0 \in T] - \Pr [X_1 \in T]| ,
\]

Consider \( T = \{ x \in S \mid \Pr [X_0 = x] \leq \Pr [X_1 = x] \} \), and notice that by this definition:

\[
\Pr [X_1 \in T] = \sum_{x \in T} \Pr [X_1 = x] \geq \sum_{x \in T} \Pr [X_0 = x] = \Pr [X_0 \in T] .
\]

Therefore \( |\Pr [X_0 \in T] - \Pr [X_1 \in T]| = \Pr [X_1 \in T] - \Pr [X_0 \in T] \), and also:

\[
\frac{1}{2} \sum_{x \in S} |\Pr [X_0 = x] - \Pr [X_1 = x]| = \frac{1}{2} \left( \sum_{x \in T} |\Pr [X_0 = x] - \Pr [X_1 = x]| + \sum_{x \in S \setminus T} |\Pr [X_0 = x] - \Pr [X_1 = x]| \right)
\]

by choice of \( T \):

\[
= \frac{1}{2} \left( \sum_{x \in T} \Pr [X_1 = x] - \Pr [X_0 = x] + \sum_{x \in S \setminus T} \Pr [X_0 = x] - \Pr [X_1 = x] \right) = \frac{1}{2} \left( \Pr [X_1 \in T] - \Pr [X_0 \in T] + \Pr [X_0 \notin T] - \Pr [X_1 \notin T] \right)
\]

1-3
\[ \frac{1}{2} \left( \Pr [X_1 \in T] - \Pr [X_0 \in T] + 1 - \Pr [X_0 \in T] - 1 + \Pr [X_1 \in T] \right) = \Pr [X_1 \in T] - \Pr [X_0 \in T] = |\Pr [X_0 \in T] - \Pr [X_1 \in T]|. \]

From both proofs we can deduce that since this selection of \( T \) got a value that is also an upper bound on the value for any \( T \), this is actually a \( T \) that brings the value to maximum, thus:

\[ \frac{1}{2} \sum_{x \in S} |\Pr [X_0 = x] - \Pr [X_1 = x]| = \max_{T \subseteq S} |\Pr [X_0 \in T] - \Pr [X_1 \in T]| . \]

\( \square \)

(c) Notice that by definition:

\[ \Delta_A ((X_0; U_n), (X_1; U_n)) = |\Pr [A(X_0; U_n) = 1] - \Pr [A(X_1; U_n) = 1]| \]

\( A \) is an indicator, therefore the probability that is gets 1 is equivalent to its expectation:

\[ \left| \sum_{x \in S, r \in \{0,1\}^n} (\Pr [X_0 = x, U_n = r'] A(x; r')) - \sum_{x \in S, r \in \{0,1\}^n} (\Pr [X_1 = x, U_n = r'] A(x; r')) \right| = \]

Since \( r' \) is chosen independently of \( x \), and uniformly:

\[ \frac{1}{2^n} \sum_{x \in S, r \in \{0,1\}^n} (\Pr [X_0 = x] A(x; r')) - \frac{1}{2^n} \sum_{x \in S, r \in \{0,1\}^n} (\Pr [X_1 = x] A(x; r')) \]

\[ \frac{1}{2^n} \sum_{r' \in \{0,1\}^n} \left( \sum_{x \in S} (\Pr [X_0 = x] A(x; r') - \Pr [X_1 = x] A(x; r')) \right) \leq \]

\[ \frac{1}{2^n} \sum_{r' \in \{0,1\}^n} \left( \sum_{x \in S} (\Pr [X_0 = x] A(x; r') - \Pr [X_1 = x] A(x; r')) \right) . \]

Notate by \( r \in \{0,1\}^n \) the value for which \( \sum_{x \in S} (\Pr [X_0 = x] A(x; r') - \Pr [X_1 = x] A(x; r')) \) is maximal, then for this \( r \):

\[ \frac{1}{2^n} \sum_{r' \in \{0,1\}^n} \left( \sum_{x \in S} (\Pr [X_0 = x] A(x; r') - \Pr [X_1 = x] A(x; r')) \right) \leq \]

\[ \frac{1}{2^n} \sum_{r' \in \{0,1\}^n} \left( \sum_{x \in S} (\Pr [X_0 = x] A(x; r') - \Pr [X_1 = x] A(x; r')) \right) = \]

\[ \sum_{x \in S} (\Pr [X_0 = x] A(x; r) - \Pr [X_1 = x] A(x; r)) = |\Pr [A(X_0; r) = 1] - \Pr [A(X_1; r) = 1]| = \]

\[ \Delta_A ((X_0; r), (X_1; r)). \]

Therefore:

\[ \Delta_A ((X_0; U_n), (X_1; U_n)) \leq \Delta_A ((X_0; r), (X_1; r)). \]

\( \square \)
3. To prove that we will show that any efficient adversary $A$ against $Y_0, Y_1$ can be translated into an efficient adversary $A'$ against $(X, S_0(X)), (X, S_1(X))$, i.e. we will show a security reduction as seen in the lectures. We will assume towards a contradiction that there exists a n.u. PPT attacker $A = \{A_n\}_{n \in \mathbb{N}}$ and polynomial $q(\cdot)$ such that for infinitely many $n \in \mathbb{N}$:

$$\Delta_{A_n} (Y_{0,n}, Y_{1,n}) \geq \frac{1}{q(n)}.$$ 

We will show that we can use $A$ to construct a n.u. PPT attacker $A' = \{A'_n\}_{n \in \mathbb{N}}$ for $(X, S_0(X)), (X, S_1(X))$.

Define the following, for some $n \in \mathbb{N}$ from our assumption:

$$H_0 = (X_n, S_0(X_n), ..., S_0(X_n))$$
$$H_1 = (X_n, S_1(X_n), S_0(X_n), ..., S_0(X_n))$$
$$\vdots$$
$$H_i = \left( X_n, S_1(X_n), ..., \underbrace{S_1(X_n), S_0(X_n), ..., S_0(X_n)}_{i} \right)$$
$$\vdots$$
$$H_{p(n)} = (X_n, S_1(X_n), ..., S_1(X_n))$$

Notice that: $H_0 = Y_{0,n}$ and $H_{p(n)} = Y_{1,n}$, thus:

$$\Delta_{A_n} (H_0, H_{p(n)}) \geq \frac{1}{q(n)}.$$ 

Notice that:

$$\frac{1}{q(n)} \leq \Delta_{A_n} (H_0, H_{p(n)}) \leq \sum_{i \in [p(n)]} \Delta_{A_n} (H_{i-1}, H_i) \leq \max_{i \in [p(n)]} \Delta_{A_n} (H_{i-1}, H_i) \cdot p(n).$$

Where the first inequality comes from our assumption and the second from triangle inequality.

For said maximal $i$, and we get: $\frac{1}{q(n)} \leq \Delta_{A_n} (H_{i-1}, H_i) \cdot p(n) \Rightarrow \Delta_{A_n} (H_{i-1}, H_i) \geq \frac{1}{q(n)p(n)}$. 

Notice that by our definition, $H_{i-1}, H_i$ only differ in the $i$th element:

- In $H_{i-1}$ we have $S_0(X_n)$,
- In $H_i$ we have $S_1(X_n)$.

Now we will construct the attacker $A'_n$: given an input $(x, S_0(x)) \leftarrow X_n, S_0(X_n)$

- Construct a new input based on $(x, S_0(x))$, by computing independently $i - 1$ values of $S_1(x)$, and $p(n) - i$ values of $S_0(x)$. This step is polynomial since both $S_0, S_1$ are PPT. The new input:

$$\left( x, S_1(x), ..., S_1(x), S_0(x), S_0(x), ..., S_0(x) \right)$$

- Return the same value that $A_n$ returns for our newly constructed input. This is also polynomial since $A_n$ is polynomial.
Notice that $A'_n$ is polynomial since each step was polynomial.

Notice that if $b = 0$, then the newly constructed input is distributed like $H_{i-1}$, and otherwise it’s distributed like $H_i$, thus:

$$
\Delta_{A'_n}((X_n,S_0(X_n)),(X_n,S_1(X_n))) = \Delta_{A_n}(H_{i-1},H_i) \geq \frac{1}{q(n)p(n)}.
$$

Thus we were able to construct an efficient adversary $A'$ using $A$, and as mentioned in the beginning this concludes our security reduction and since we know $X, S_0(X) \approx_c X, S_1(X)$, we get by the reduction that $Y_0 \approx_c Y_1$.

\[\square\]

**Bonus**

Let $(E,D)$ be a computationally secure encryption scheme for keys of size $n$ and messages of size $2n$, as we know exists by the assumption.

Define:

- $X_n = \{ct \mid sk \leftarrow \{0,1\}^n, b \leftarrow \{0,1\}, ct \leftarrow E_{sk}(m_b)\}$ where $m_0, m_1$ are two messages that can be distinguished by an adversary as described in question 1,
- $S_0(X_n)$ is the uniform distribution over 0,1,
- $S_1(X_n)$ is a non efficient deterministic algorithm that outputs 1 if $X_n = E_{sk}(m_1)$ and 0 otherwise, we saw in the lectures\(^3\) that there exists such algorithm that is right with probability of at least $1 - 2^{-n}$.

Notice that $X, S_0(X) \approx_c X, S_1(X)$ by the fact that the encryption scheme is computationally secure, because if we assume towards a contradiction that there exists a n.u. PPT attacker $A = \{A_n\}_{n \in \mathbb{N}}$ and polynomial $q(\cdot)$ such that for infinitely many $n \in \mathbb{N}$:

$$
\Delta_{A_n}((X_n,S_0(X_n)),(X_n,S_1(X_n))) \geq \frac{1}{q(n)},
$$

then we can construct an efficient adversary $A'$ against $(E,D)$, and differentiate between encryption of $m_0,m_1$ by simply applying $A$ on $(ct,0)$. If by $A : (ct,0) \in X_n, S_1(X_n)$, we will return 0, and otherwise we will return 1.

Our newly constructed $A$ will choose the correct message with probability of at least $0.99/q(n)$ since $1/q(n)$ is the probability of choosing the correct pair $X_n, S_n(X_n)$, and since $S_1$ is correct with probability $1 - 2^{-n} \geq 0.99$.\(^4\)

Thus we showed a computational reduction between differentiating $X, S_0(X), X, S_1(X)$ and breaking the encryption scheme. And since we know that the scheme is computationally secure: $X, S_0(X) \approx_c X, S_1(X)$.

Now, we will show an efficient algorithm $A$ to differentiate between $Y_0, Y_1$:

Given an input $(X_n,S_0(X_n),...,S_0(X_n))$, $A_n$ returns 1 if all results of $S_0(X_n)$ are identical and 0 otherwise. By definition of $S_0, S_1$, and since $S_1$ is deterministic:

$$
\Pr[A((X_n,S_0(X_n),...,S_0(X_n))) = 1 \mid b = 1] = \Pr[A((X_n,S_1(X_n),...,S_1(X_n))) = 1] = 1
$$

$$
\Pr[A((X_n,S_0(X_n),...,S_0(X_n))) = 1 \mid b = 0] = \Pr[A((X_n,S_0(X_n),...,S_0(X_n))) = 1] \leq 2^{-p(n)+1}
\Rightarrow \Delta_{A_n}((X_n,S_0(X_n)),(X_n,S_1(X_n))) \geq 1 - 2^{-p(n)+1}.
$$

\(^3\)We assume w.l.o.g. that $E$ is deterministic but we saw in question 1 that all steps here are also correct if $E$ uses randomization.

\(^4\)Starting from say $n \geq 6$. 
Since we can see that $\lim_{n \to \infty} 1 - 2^{-p(n)+1} = 1$, we can safely say that there is a place $n'$ from which $1 - 2^{-p(n)+1} \geq 1/n$, therefore we can say (at the very least) that there are infinitely many $n \in \mathbb{N}$ for which:

$$\Delta_{A_n}((X_n, S_0(X_n)), (X_n, S_1(X_n))) \geq 1/n,$$

thus it cannot hold that: $Y_0 \approx_c Y_1$

$\square$