6.857 Homework	**Problem Set 3**	# 3-2. IND-CCA
		April 15, 2014

Theorem: Bob's method E is *not* IND-CCA secure.

Proof: The adversary picks $m_0 = 0^x, m_1 = 1^x$ for large $x \geq 3 \cdot 128$ in phase I. Then $y = E_{K_1,K_2}(m_d)$. Let $z = y$ with the first bit flipped. Since $z \neq y$, the adversary is allowed to ask for $D_{K_1,K_2}(z)$ in phase II. This correctly gives the first 128-bit block of m_d, revealing d (zeroes if $d = 0$ or ones if $d = 1$). Therefore, the adversary wins the game.

Why does this work? Consider the steps of E, where m_d is divided into n 128-bit blocks ($n \geq 3$):

1. Start with $m_d = m_1, \ldots, m_n$.
2. $\mathsf{EncCBC}_{K_1}(m_1, \ldots, m_n) = IV^{(1)}, C_1^{(1)}, \ldots, C_n^{(1)}$.
3. $\mathsf{Rev}(IV^{(1)}, C_1^{(1)}, \ldots, C_n^{(1)}) = C_n^{(1)}, \ldots, C_1^{(1)}, IV^{(1)}$.
4. $\mathsf{EncCBC}_{K_2}(C_n^{(1)}, \ldots, C_1^{(1)}, IV^{(1)}) = IV^{(2)}, C_1^{(2)}, \ldots, C_n^{(2)}, C_{n+1}^{(2)}$.
5. End with $IV^{(2)}, C_1^{(2)}, \ldots, C_n^{(2)}, C_{n+1}^{(2)} = y$.

Now, consider the steps of D, which reverses E.

1. Start with $y = IV^{(2)}, C_1^{(2)}, \ldots, C_n^{(2)}, C_{n+1}^{(2)}$.
2. $\mathsf{DecCBC}_{K_2}(IV^{(2)}, C_1^{(2)}, \ldots, C_n^{(2)}, C_{n+1}^{(2)}) = C_n^{(1)}, \ldots, C_1^{(1)}, IV^{(1)}$.
3. $\mathsf{Rev}(C_n^{(1)}, \ldots, C_1^{(1)}, IV^{(1)}) = IV^{(1)}, C_1^{(1)}, \ldots, C_n^{(1)}$.
4. $\mathsf{DecCBC}_{K_1}(IV^{(1)}, C_1^{(1)}, \ldots, C_n^{(1)}) = m_1, \ldots, m_n$.
5. End with $m_1, \ldots, m_n = m_d$.

Finally, consider the steps of D when the input is z instead of y (the first bit is flipped). Denote any changed blocks in red. As we observed in Lecture 9, the bit flip only affects the decryption of the current block and the next block, since each decrypted block only depends on C_i and C_{i-1} (and only the first block depends on IV).

1. Start with $z = {\color{red}IV^{(2)}}, C_1^{(2)}, \ldots, C_n^{(2)}, C_{n+1}^{(2)}$.
2. $\mathsf{DecCBC}_{K_2}({\color{red}IV^{(2)}}, C_1^{(2)}, \ldots, C_n^{(2)}, C_{n+1}^{(2)}) = {\color{red}C_n^{(1)}}, \ldots, C_1^{(1)}, IV^{(1)}$.
3. $\mathsf{Rev}({\color{red}C_n^{(1)}}, \ldots, C_1^{(1)}, IV^{(1)}) = IV^{(1)}, C_1^{(1)}, \ldots, {\color{red}C_n^{(1)}}$.
4. $\mathsf{DecCBC}_{K_1}(IV^{(1)}, C_1^{(1)}, \ldots, {\color{red}C_n^{(1)}}) = m_1, \ldots, {\color{red}m_n}$.
5. End with $m_1, \ldots, {\color{red}m_n}$.

Therefore, the first block m_1 of m_d is correct, revealing d.