Problem7: CPA Game
In our solution, we just consider the first block of CBC.

- $i = 1$: Victor chooses $m_{1,0} = 0^n$ and $m_{1,1} = 0^n$. After Alice's encryption, Victor obtains $c_1 = c_{1,0} = c_{1,1} = (IV \| E(IV))$

After the first iteration, we know IV and $E(IV)$

- $i = 2$: Victor chooses $m_{2,0} = 0^n$ and $m_{2,1} = IV \oplus E(IV)$. After Alice's encryption, Victor obtains two possible c_2 corresponding to $m_{2,0}$ and $m_{2,1}$

$$c_{2,0} = (E(IV) \| E^2(IV)),$$
$$c_{2,1} = (E(IV) \| E(IV))$$

Because Victor already knows $E(IV)$, he can realise the ciphertext c_2 sent to him is the encryption of $m_{2,0}$ or $m_{2,1}$. In other words, he knows exactly which is the bit of b.

<u>CPA Game Generalize</u>
Notation:

1. Given a message M of the i^{th} query for bit b:
   $M_{i,b} = \{m_1, m_2, ..., m_k \ : \ m_j \in F_2^n\}$
   We call the j^{th} block (m_j) of the i^{th} message ($M_{i,b}$) as $M_{i,b}[j]$
2. Given a ciphertext C of the i^{th} query for bit b:
   $C_{i,b} = \{c_0, c_1, ..., c_k \ : \ c_j \in F_2^n\}$
   We call the j^{th} block (c_j) of the i^{th} ciphertext ($C_{i,b}$) as $C_{i,b}[j]$ or $C_i[j]$

From the property of Alice encryption, we have: $C_i[0] = C_{i-1}[k]$ and $C_1[0] = IV$

We can generalize for any 2 sequential query with message M of k blocks (k$\geq$1).

- For any i^{th} query, Victor send:
  $$M_i = M_{i,0} = M_{i,1} = \{M_i[1] \| ... \| M_i[k-1] \| M_i[k]\}$$
  Victor will receive: $C_i = C_{i,0} = C_{i,1}$
  $$C_i = \{C_i[0] \| ... \| C_i[k-1] \| C_i[k]\}$$
- For the $(i+1)^{th}$ query, Victor modifies the 1st block the message M_{i+1}:
  $M_{i+1,1}[1] = C_i[k] \oplus C_i[k-1] \oplus M_i[k]$
  $M_{i+1,0}[1] \neq M_{i+1,1}[1]$
  Then, Victor has two possible of $C_{i+1}[1]$:
  $C_{i+1,0}[1] = E(C_{i+1}[0] \oplus M_{i+1,0}[1])$
  $= E(C_i[k] \oplus M_{i+1,0}[1])$

$$
\begin{aligned}
C_{i+1,\,1}[1] &= E(C_{i+1}[0] \oplus M_{i+1,\,1}[1]) \\
&= E(C_i[k] \oplus M_{i+1,\,1}[1]) \\
&= E(C_i[k] \oplus C_i[k] \oplus C_i[k-1] \oplus M_i[k]) \\
&= E(C_i[k-1] \oplus M_i[k]) \\
&= C_i[k]
\end{aligned}
$$

Because Victor knew $C_i[k]$, based on the value of $C_{i+1}[1]$, Victor can realise whether the ciphertext C_{i+1} was created using $M_{i+1,\,0}$ or $M_{i+1,\,1}$. Therefore, Victor knows exactly the value of bit b.