1. Practitioners of CBC mode are often suspicious of the IV, and don’t believe that it can be just given out as part of the ciphertext. An natural way to try to hide the IV is to send it through the block cipher before including it in the ciphertext. In other words, we modify CBC encryption as follows:

\[
\text{Enc}(k, m_1 \cdots m_\ell): \\
c_0 \leftarrow \{0, 1\}^h: \\
\text{for } i = 1 \text{ to } \ell: \\
c_i := F(k, m_i \oplus c_{i-1}) \\
c_0' := F(k, c_0) \\
\text{return } c_0', c_1 \cdots c_\ell
\]

To decrypt, we first compute \(c_0 := F^{-1}(k, c_0')\) and proceed as in usual CBC decryption.

Show that the resulting scheme is not CPA secure. Describe a successful distinguisher and compute its advantage.

Note: We’re talking about CPA in this problem, not CCA!

2. It’s obviously secure to encrypt the same thing twice, right? Suppose I take an existing encryption scheme \(\Sigma\) and I define a new encryption scheme \(\Sigma'\) which basically says “encrypt twice under \(\Sigma\)”

\[
\Sigma'.\text{KeyGen}: \\
\hat{k} \leftarrow \Sigma.\text{KeyGen} \\
\text{return } \hat{k}
\]

\[
\Sigma'.\text{Enc}(k, m): \\
c_1 := \Sigma.\text{Enc}(k, m) \\
c_2 := \Sigma.\text{Enc}(k, m) \\
\text{return } (c_1, c_2)
\]

\[
\Sigma'.\text{Dec}(k, (c_1, c_2)): \\
m_1 := \Sigma.\text{Dec}(k, c_1) \\
m_2 := \Sigma.\text{Dec}(k, c_2) \\
\text{if } m_1 = m_2 \text{ then return } m_1 \\
\text{else return } \text{err}
\]

(a) Prove that if \(\Sigma\) has CPA security, then so does \(\Sigma'\).

(b) Show that \(\Sigma'\) does not have CCA security (even if \(\Sigma\) does)!

\text{Hint:} In the attack I have in mind, you have to call \text{CHALLENGE} twice, then do something clever with the results, then ask for something to be decrypted.

3. Describe the \text{Dec} algorithm that goes with this encryption algorithm. Show that the scheme is not CCA secure:

\[
\text{Enc}(k, m): \\
r \leftarrow \{0, 1\}^h \\
x := F(k, m \oplus r) \oplus r \\
\text{return } (r, x)
\]

\text{Hint:} How can you modify a ciphertext so that something predictable gets fed into \(F^{-1}\) during decryption?

continues on next page
Refer to the text for a definition of CCA$ security. Prove that an encryption scheme $\Sigma$ has CCA$ security if and only if the following two libraries are indistinguishable. In other words, these two libraries would be an equivalent way to define CCA$ security:

Note: In $L_{\text{left}}$, the adversary can obtain the decryption of any ciphertext via $\text{Dec}$. In $L_{\text{right}}$, the $\text{Dec}$ subroutine is “patched” (via $D$) to give reasonable answers to ciphertexts generated in $\text{Challenge}$. 