1. Here is an insecure technique for ciphertext stealing, that was actually used in the wild. Suppose the final plaintext block $m_\ell$ is $\text{blen} - j$ bits long. Rather than padding the final block with zeroes, it is padded with the last $j$ bits of ciphertext block $c_{\ell-1}$. Then the padded block $m_\ell$ is sent through the PRP to produce the final ciphertext block $c_\ell$. Since the final $j$ bits of $c_{\ell-1}$ are recoverable from $c_\ell$, they can be discarded.

If the final block of plaintext is already $\text{blen}$ bits long, then standard CBC mode is used.

Show that the scheme does not satisfy CPA$^\$ security. Describe a distinguisher and compute its advantage.

*Hint:* ask for several encryptions of plaintexts whose last block is $\text{blen} - 1$ bits long.

2. Show that the following block cipher mode is not CPA/CPA$^\$-secure. Describe a successful distinguisher and compute its advantage. You can attack either CPA security or CPA$^\$ security, I don’t care. Just make it obvious what property you are attacking. Here $F$ is a
3. Alice doesn’t trust how CBC mode reveals the IV as part of the ciphertext. She thinks it would be preferable to hide the IV. She proposes to send the IV through the block cipher before including it in the ciphertext. In other words, she modifies CBC encryption as follows:

To decrypt, just compute \( c_0 := F^{-1}(k, c'_0) \) and proceed as in usual CBC decryption.

(a) Show that the resulting scheme no longer satisfies CPA/CPA$ security. Describe a successful distinguisher and compute its advantage. You can attack either CPA security or CPA$ security, I don’t care. Just make it obvious what property you are attacking.

(b) Show that if we instead compute \( c'_0 = F(k', c_0) \), where \( k' \) is an independently chosen key (so the modified CBC mode now has a key \( (k, k') \)), the resulting scheme does still achieve CPA$ security. Your security proof can use the fact that standard CBC encryption has CPA$ security.

grad. In all of the CPA-secure encryption schemes that we’ve ever seen, ciphertexts are at least \( \lambda \) bits longer than plaintexts. This problem shows that such ciphertext expansion is essentially unavoidable for CPA security.

Let \( \Sigma \) be an encryption scheme with plaintext space \( M = \{0,1\}^n \) and ciphertext space \( C = \{0,1\}^{n+\ell} \). Show that there exists a distinguisher that distinguishes the two CPA libraries with advantage \( \Omega(1/2^\ell) \).

Hint: As a warmup, consider the case where each plaintext has exactly \( 2^\ell \) possible ciphertexts. However, this need not be true in general. For the general case, choose a random plaintext \( m \) and argue that with “good probability” (that you should precisely quantify) \( m \) has at most \( 2^{\ell+1} \) possible ciphertexts.