CS 427/519: Homework 4

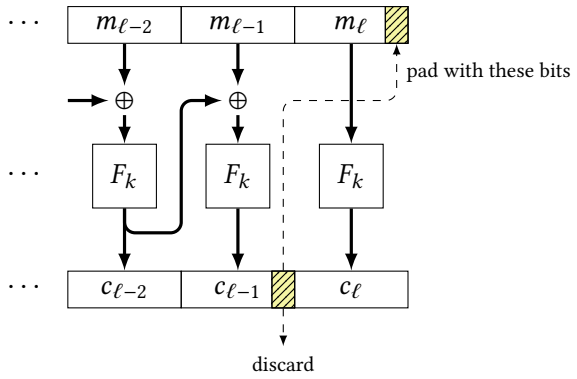
Due: Monday February 12, 10pm; **typed** and **submitted electronically**.

Important notes for this homework and all future ones:

- When asked to show that something is **secure**, please clarify what libraries you are going to show indistinguishable. List a sequence of hybrid libraries and briefly justify each step (that two consecutive hybrids are indistinguishable).
- When asked to show that something is **insecure**, please clarify what libraries you are going to distinguish. Explicitly write the code of the distinguisher / calling program. Explicitly derive the output probability of the distinguisher in the presence of each library.

1. Here is an insecure technique for ciphertext stealing, that was actually used in the wild. Suppose the final plaintext block m_ℓ is 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_ℓ is sent through the PRP to produce the final ciphertext block c_ℓ. Since the final j bits of $c_{\ell-1}$ are recoverable from c_ℓ, they can be discarded.

   If the final block of plaintext is already 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 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

secure PRP with block length blen = λ.

```
Enc(k, m_1 ··· m_ℓ):
  c_0 ← {0,1}^λ
  r_0 := c_0
  for i = 1 to ℓ:
    r_i := r_{i−1} ⊕ m_i
    c_i := F(k, r_i)
  return c_0 ··· c_ℓ
```

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:

```
Enc(k, m_1 ··· m_ℓ):
  c_0 ← {0,1}^blen:
  for i = 1 to ℓ:
    c_i := F(k, m_i ⊕ c_{i−1})
  c'_0 := F(k, c_0)
  return c'_0 c_1 ··· c_ℓ
```

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 λ bits longer than plaintexts. This problem shows that such **ciphertext expansion** is essentially unavoidable for CPA security.

Let Σ be an encryption scheme with plaintext space $\mathcal{M} = \{0,1\}^n$ 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^ℓ 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.