Cryptography: HW3

Due electronically (via TEACH) on **Friday** Feb 5

1. Show that any function F that is a 2-round keyed Feistel cipher **cannot** be a secure PRP. Your distinguisher should work without knowing what the round functions are, and the attack should work with different (independent) round functions for the 2 rounds.

   Hint: Make two queries, where the second query depends on the answer to the first. With carefully chosen queries, it is possible to identify a property that is always satisfied by a 2-round Feistel network but that is rarely satisfied by a random function.

2. Let F be a secure PRP with blocklength $\mathsf{blen} = \lambda$, and consider the block cipher mode below:

```
$\mathsf{Enc}(k, m_1 \cdots m_\ell)$:
  $c_0 \leftarrow \{0,1\}^\lambda$
  $m_0 := c_0$
  for $i = 1$ to $\ell$:
    $c_i := F(k, m_i) \oplus m_{i-1}$
  return $c_0 \cdots c_\ell$
```

   (a) Describe the corresponding decryption mode.

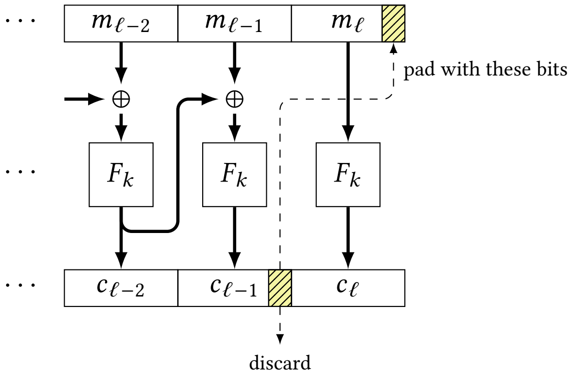
   (b) Show that the mode does not have CPA$ security by describing a successful distinguisher and computing its advantage.

(continues on next page)

3. In this problem we consider a different technique for ciphertext stealing in CBC mode. You will show that it is insecure.

   Suppose the final plaintext block m_ℓ is $\mathsf{blen} - j$ 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 $\mathsf{blen} - 1$ bits long.

4. Block cipher modes generally require an IV that is chosen uniformly. In this problem we discuss what happens if the adversary has influence over the choice of IV.

   (a) Describe a modification to the CPA$ security definition that allows the adversary to choose the IV that is used (in addition to choosing the plaintext), *but is not allowed to re-use an IV.*

   (b) Show that CBC mode does not satisfy CPA$ security against chosen-IV attacks. Describe an explicit distinguisher for your modified security definition, and compute its advantage.