Cryptography: HW4

Due electronically (via TEACH) on Friday Feb 19

1. Let $F$ be a secure PRP with blocklength $\text{blen} = \lambda$. Consider the encryption scheme below:

<table>
<thead>
<tr>
<th>$K$</th>
<th>${0,1}^{\lambda}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$M$</td>
<td>${0,1}^{\lambda}$</td>
</tr>
<tr>
<td>$C$</td>
<td>$({0,1}^{\lambda})^2$</td>
</tr>
</tbody>
</table>

**KeyGen:**
\[ k \leftarrow \{0,1\}^{\lambda} \]
\[ \text{return } k \]

**Enc($k$, $m$):**
\[ r \leftarrow \{0,1\}^{\lambda} \]
\[ s := F(k, r \oplus m) \oplus r \]
\[ \text{return } (r, s) \]

(a) Show the corresponding decryption algorithm.

(b) Show that the scheme does **not** have CCA security. Describe a successful distinguisher and compute its advantage.

2. Let $F$ be a secure PRF with $\text{in} = \text{out} = \lambda$. Show that the following scheme is **not** a secure MAC (describe a successful distinguisher and compute its advantage).

**MAC($k$, $m_1 \cdots m_\ell$):**
\[ // \text{each } m_i \text{ is } \lambda \text{ bits} \]
\[ t := \text{empty string} \]
\[ \text{for } i = 1 \text{ to } \ell: \]
\[ t := t||F(k, m_i) \]
\[ \text{return } t \]

3. CBC-MAC is secure when the scheme is restricted to messages of a single length. Show that CBC-MAC is insecure when applied to messages of different lengths.

*Hint:* request MACs of two single-block messages, then use the results to forge the MAC of a two-block message.

4. When we combine different cryptographic ingredients (e.g., combining a CPA-secure encryption scheme with a MAC to obtain a CCA-secure scheme) we generally require the two ingredients to use separate, independent keys. It would be more convenient if the entire scheme just used a single $\lambda$-bit key.

(a) Suppose we are using Encrypt-then-MAC, where both the encryption scheme and MAC have keys that are $\lambda$ bits long. Refer to the proof of security in the notes (11.4) and **describe where it breaks down** when we modify Encrypt-then-MAC to use the same key for both the encryption & MAC components:

| KeyGen: | $k \leftarrow \{0,1\}^{\lambda}$ | return $k$ |
| Enc($k$, $m$): | $c \leftarrow E.\text{Enc}(k, m)$ | $t := M.\text{MAC}(k, c)$ | return $(c, t)$ |
| Dec($k$, $(c, t)$): | \begin{align*} &\text{if } t \neq M.\text{MAC}(k, c): \text{ return err} \\ &\text{return } E.\text{Dec}(k, c) \end{align*} |

(b) While Encrypt-then-MAC requires independent keys $k_e$ and $k_m$ for the two components, show that they can both be **derived** from a single key using a PRF.
In more detail, let $F$ be a PRF with $\text{in} = 1$ and $\text{out} = \lambda$. Prove that the following modified Encrypt-then-MAC construction is CCA-secure:

```
KeyGen:
$k^* \leftarrow \{0,1\}^\lambda$
return $k^*$

Enc($k^*, m$):
$k_e := F(k^*, 0)$
$k_m := F(k^*, 1)$
c $\leftarrow$ E.Enc($k_e, m$)
t $:= M$.MAC($k_m, c$)
return $(c, t)$

Dec($k^*, (c, t)$):
$k_e := F(k^*, 0)$
$k_m := F(k^*, 1)$
if $t \neq M$.MAC($k_m, c$):
  return $err$
return $E$.Dec($k_e, c$)
```

You should not have to re-prove all the tedious steps of the Encrypt-then-MAC security proof. Rather, you should apply the security of the PRF in order to reach the original Encrypt-then-MAC construction, whose security we already proved (so you don’t have to repeat).