Cryptography: HW4

Due electronically (via TEACH) on **Friday** Feb 19

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

$$\begin{array}{lll} \mathcal{K} = \{0,1\}^\lambda & \underline{\text{KeyGen}:} & \underline{\text{Enc}(k,m):} \\ \mathcal{M} = \{0,1\}^\lambda & \quad k \leftarrow \{0,1\}^\lambda & \quad r \leftarrow \{0,1\}^\lambda \\ \mathcal{C} = (\{0,1\}^\lambda)^2 & \quad \text{return } k & \quad s := F(k, r \oplus m) \oplus r \\ & & \quad \text{return } (r,s) \end{array}$$

   (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 in $=$ out $= \lambda$. Show that the following scheme is **not** a secure MAC (describe a successful distinguisher and compute its advantage).

$$\begin{array}{l} \underline{\text{MAC}(k, m_1 \cdots m_\ell):} \\ \quad \textit{// each } m_i \textit{ is } \lambda \textit{ bits} \\ \quad t := \text{empty string} \\ \quad \text{for } i = 1 \text{ to } \ell: \\ \quad\quad t := t \| F(k, m_i) \\ \quad \text{return } t \end{array}$$

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 λ-bit key.

   (a) Suppose we are using Encrypt-then-MAC, where both the encryption scheme and MAC have keys that are λ 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:

$$\begin{array}{lll} \underline{\text{KeyGen}:} & \underline{\text{Enc}(\boxed{k}, m):} & \underline{\text{Dec}(\boxed{k}, (c,t)):} \\ \quad \boxed{k \leftarrow \{0,1\}^\lambda} & \quad c \leftarrow E.\text{Enc}(\boxed{k}, m) & \quad \text{if } t \neq M.\text{MAC}(\boxed{k}, c): \\ \quad \text{return } k & \quad t := M.\text{MAC}(\boxed{k}, c) & \quad\quad \text{return } \texttt{err} \\ & \quad \text{return } (c,t) & \quad \text{return } E.\text{Dec}(\boxed{k}, c) \end{array}$$

   (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 $\mathsf{in} = 1$ and $\mathsf{out} = \lambda$. Prove that the following modified Encrypt-then-MAC construction is CCA-secure:

KeyGen:	Enc(k^*, m):	Dec(k^*, (c,t)):
$k^* \leftarrow \{0,1\}^\lambda$ return k^*	$k_\mathsf{e} := F(k^*, 0)$ $k_\mathsf{m} := F(k^*, 1)$ $c \leftarrow E.\mathsf{Enc}(k_\mathsf{e}, m)$ $t := M.\mathsf{MAC}(k_\mathsf{m}, c)$ return (c, t)	$k_\mathsf{e} := F(k^*, 0)$ $k_\mathsf{m} := F(k^*, 1)$ if $t \neq M.\mathsf{MAC}(k_\mathsf{m}, c)$: return err return $E.\mathsf{Dec}(k_\mathsf{e}, c)$

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).