Problem Set 5

Due: Monday November 2, 2009, in class.

Collaboration is not allowed on this problem set. See the course information sheet for collaboration rules.

Problem 1. [40 points] Let $\mathcal{K}$ be the key generation algorithm that returns a random 128-bit AES key K, and let $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be the symmetric encryption scheme whose encryption and decryption algorithms are as follows:

```
algorithm E_K(M)
    if |M| ≠ 512 then return ⊥
    M[1]...M[4] ← M
    C_e[0] ←$ {0,1}^128 ; C_m[0] ← 0^128
    for i = 1,...,4 do
        C_e[i] ← E_K(C_e[i−1] ⊕ M[i])
        C_m[i] ← E_K(C_m[i−1] ⊕ M[i])
    C_e ← C_e[0]C_e[1]C_e[2]C_e[3]C_e[4]
    T ← C_m[4]
    return (C_e, T)

algorithm D_K((C_e, T))
    if |C_e| ≠ 640 then return ⊥
    C_m[0] ← 0^128
    for i = 1,...,4 do
        M[i] ← E_K^{−1}(C_e[i]) ⊕ C_e[i−1]
        C_m[i] ← E_K(C_m[i−1] ⊕ M[i])
    if C_m[4] ≠ T then return ⊥
    return M
```

Above, $X[i]$ denotes the i-th 128-bit block of a string whose length is a multiple of 128, and $M[1] \ldots M[4] \leftarrow M$ means we break M into 128-bit blocks.

1. **[30 points]** For each of the following notions of security, say whether the scheme is SECURE or INSECURE and justify your answer: INT-PTXT, INT-CTXT, IND-CPA, IND-CCA.

2. **[10 points]** Discuss this scheme from the point of view of being an Encrypt-and-MAC construction. Is it? For which choices of Encrypt and MAC? How do you reconcile your findings about its security with what we know about the security of this construction?

Problem 2. [40 points] Let $\mathcal{SE} = (\mathcal{K}_e, \mathcal{E}, \mathcal{D})$ be an IND-CPA symmetric encryption scheme, and $\Pi = (\mathcal{K}_m, \mathcal{T}, \mathcal{V})$ a SUF-CMA MAC. Let $\overline{\mathcal{SE}} = (\mathcal{K}, \overline{\mathcal{E}}, \overline{\mathcal{D}})$ be the symmetric encryption scheme whose algorithms are as follows:

Game G_0, $\boxed{G_1}$

procedure Initialize

$K_1 \xleftarrow{\$} \mathcal{K}_e$; $K_2 \xleftarrow{\$} \mathcal{K}_m$; $b \xleftarrow{\$} \{0,1\}$; $S \leftarrow \emptyset$

procedure LR(M_0, M_1)

$C \xleftarrow{\$} \mathcal{E}(K_1, M_b)$; $T \xleftarrow{\$} \mathcal{T}(K_2, C)$; $S \leftarrow S \cup \{(C,T)\}$; Return (C,T)

procedure Dec$((C,T))$

If $(C,T) \in S$ then return $\perp$
$M \leftarrow \perp$
If $\mathcal{V}(K_2, C, T) = 1$ then
  $\mathsf{bad} \leftarrow \mathsf{true}$; $\boxed{M \leftarrow \mathcal{D}(K_1, C)}$
Return M

procedure Finalize(b')

return $(b = b')$

Figure 1: Game G_1 includes the boxed code and game G_0 does not.

algorithm $\overline{\mathcal{K}}$ $K_1 \xleftarrow{\$} \mathcal{K}_e$ $K_2 \xleftarrow{\$} \mathcal{K}_m$ Return $K_1 \parallel K_2$	algorithm $\overline{\mathcal{E}}(K_1 \parallel K_2, M)$ $C \xleftarrow{\$} \mathcal{E}(K_1, M)$ $T \xleftarrow{\$} \mathcal{T}(K_2, C)$ Return (C,T)	algorithm $\overline{\mathcal{D}}(K_1 \parallel K_2, (C,T))$ If $\mathcal{V}(K_2, C, T) = 0$ then return $\perp$ $M \leftarrow \mathcal{D}(K_1, C)$ Return M

Show that $\overline{\mathcal{SE}}$ is IND-CCA by establishing the following.

Theorem: Let A be an ind-cca-adversary against $\overline{\mathcal{SE}}$ that makes at most q_e **LR** queries and at most q_d **Dec** queries. Then there is an ind-cpa-adversary $A_{\mathcal{SE}}$ and a uf-cma-adversary A_Π such that

$$\mathbf{Adv}^{\text{ind-cca}}_{\overline{\mathcal{SE}}}(A) \;\leq\; \mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A_{\mathcal{SE}}) + 2 \cdot \mathbf{Adv}^{\text{suf-cma}}_{\Pi}(A_\Pi) \; . \tag{1}$$

Furthermore the number of **LR** queries made by $A_{\mathcal{SE}}$ is at most q_e, the number of **Tag** queries made by A_Π is at most q_e, the number of **Verify** oracle queries made by A_Π is at most q_d, and both constructed adversaries have running time that of A plus minor overhead.

Your proof should use a game sequence that includes the games G_0, G_1 of Fig. 1.
