Computer Sciences, UW–Madison — Spring 2012
CS 838: Applied Cryptography — **Instructor:** Thomas Ristenpart
Problem Set 2 — March 20, 2012

Problem Set 2

Due: Tuesday April 10, 2012.

You may discuss the problem set with classmates, but must write up problem solutions individually. If you discuss a problem with someone, indicate it clearly at the beginning of the problem's solution. I will check that you turned it in and attempted the problems.

Problem 1. Let $E: \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher and let algorithm $\mathcal{K}$ return $K \stackrel{\$}{\leftarrow} \{0,1\}^k$. Assume messages to be encrypted have length $\ell < n$. Let $\mathcal{E}$ be the following encryption algorithm:

algorithm $\mathcal{E}_K(M)$
  if $|M| \neq \ell$ then return $\perp$ // Only encrypts ℓ-bit messages
  $R \stackrel{\$}{\leftarrow} \{0,1\}^{n-\ell}$
  $C \leftarrow E_K(R \,\|\, M)$
  return C

Above, "$x \,\|\, y$" denotes the concatenation of strings x and y.

1. Specify a decryption algorithm $\mathcal{D}$ such that $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is a symmetric encryption scheme providing correct decryption.

2. Give the best attack you can on this scheme. Given an even number q, your attack should take the form of an ind-cpa adversary A that makes q oracle queries and has running time around that for $O(q)$ applications of E. Specify $\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A)$ as a function of q, n, ℓ. Letting $n = 128$, make a table showing, for values $\ell = 1, 16, 32, 64, 96$, the smallest value of q for which the advantage is at least $1/4$. For the analysis, you may find Lemma A.1 below useful.

3. Give a reduction of the IND-CPA security of $\mathcal{SE}$ to the PRF security of E. This means you must state a theorem that upper bounds the ind-cpa advantage of a given ind-cpa adversary A as a function of the prf-advantage of a constructed prf-adversary B and (possibly) n, ℓ and the number q of LR-queries made by A. This is analogous to results we have seen in class for CTRC and CBC\$ encryption. Prove your theorem using a game sequence.

4. As a result of the above, do you consider the scheme to be secure or insecure? Discuss this for $E = \mathsf{AES}$ and $\ell = 1, 16, 32, 64, 96$.

Problem 2. Let E: $\{0,1\}^k \times \{0,1\}^l \to \{0,1\}^l$ be a block cipher. Let D be the set of all strings whose length is a positive multiple of l.

1. Define the hash function H_1: $\{0,1\}^k \times D \to \{0,1\}^l$ via the CBC construction, as follows:

algorithm $H_1(K, M)$
  $M[1]M[2]\ldots M[n] \leftarrow M$
  $C[0] \leftarrow 0^l$
  For $i = 1, \ldots, n$ do $C[i] \leftarrow E(K, C[i-1] \oplus M[i])$
  Return $C[n]$

Show that H_1 is not collision-resistant.

2. Define the hash function H_2: $\{0,1\}^k \times D \to \{0,1\}^l$ as follows:

algorithm $H_2(K, M)$
  $M[1]M[2]\ldots M[n] \leftarrow M$
  $C[0] \leftarrow 0^l$
  For $i = 1, \ldots, n$ do $B[i] \leftarrow E(K, C[i-1] \oplus M[i])$; $C[i] \leftarrow E(K, B[i] \oplus M[i])$
  Return $C[n]$

Is H_2 collision-resistant? If you say NO, present an attack. If YES, explain your answer, or, better yet, prove it.

Above, $M[1]M[2]\ldots M[n] \leftarrow M$ means we break M into l-bit blocks, with $M[i]$ denoting the i-th block. For any attack (adversary) you provide, state its time-complexity. (The amount of credit you get depends on how low this is.)

Problem 4. Let E denote AES. 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 $\mathcal{E}_K(M)$	algorithm $\mathcal{D}_K((C_e, T))$
if $\lvert M \rvert \neq 512$ then return $\perp$	if $\lvert C_e \rvert \neq 640$ then return $\perp$
$M[1]\ldots M[4] \leftarrow M$	$C_m[0] \leftarrow 0^{128}$
$C_e[0] \xleftarrow{\$} \{0,1\}^{128}$; $C_m[0] \leftarrow 0^{128}$	for $i = 1, \ldots, 4$ do
for $i = 1, \ldots, 4$ do	$M[i] \leftarrow E_K^{-1}(C_e[i]) \oplus C_e[i-1]$
$C_e[i] \leftarrow E_K(C_e[i-1] \oplus M[i])$	$C_m[i] \leftarrow E_K(C_m[i-1] \oplus M[i])$
$C_m[i] \leftarrow E_K(C_m[i-1] \oplus M[i])$	if $C_m[4] \neq T$ then return $\perp$
$C_e \leftarrow C_e[0]C_e[1]C_e[2]C_e[3]C_e[4]$	return M
$T \leftarrow C_m[4]$	
return (C_e, T)	

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. For each of the following notions of security, say whether the scheme is SECURE or INSE-

main $\underline{\text{SUFCMA}_{\mathcal{MA}}}$ $K \xleftarrow{\$} \mathcal{K}; S \leftarrow \emptyset$ $A^{\textbf{Tag},\textbf{Verify}}$ Return win	**procedure** $\underline{\textbf{Verify}(M,T)}$ $d \leftarrow \mathcal{V}_K(M,T)$ If $(d = 1 \wedge (M,T) \notin S)$ then win $\leftarrow$ true return d **procedure** $\underline{\textbf{Tag}(M)}$ $T \xleftarrow{\$} \mathcal{T}_K(M)$ $S \leftarrow S \cup \{(M,T)\}$ return T

Figure 1: The $\text{SUFCMA}_{\mathcal{MA}}$ game.

CURE and justify your answer: INT-PTXT, INT-CTXT, IND-CPA, IND-CCA.

2. 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 5. Let $\mathcal{SE} = (\mathcal{K}_e, \mathcal{E}, \mathcal{D})$ be an IND-CPA symmetric encryption scheme, and $\mathcal{MA} = (\mathcal{K}_m, \mathcal{T}, \mathcal{V})$ a MAC. Let $\overline{\mathcal{SE}} = (\mathcal{K}, \overline{\mathcal{E}}, \overline{\mathcal{D}})$ be the symmetric encryption scheme whose algorithms are as follows:

algorithm $\mathcal{K}$ $K_1 \xleftarrow{\$} \mathcal{K}_e$ $K_2 \xleftarrow{\$} \mathcal{K}_m$ 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

1. SUF-CMA is a strengthening of the notion UF-CMA given in class; it is shown in Fig. 1. The suf-cma advantage of adversary A is

$$\mathbf{Adv}^{\text{suf-cma}}_{\mathcal{MA}}(A) = \Pr\left[\text{SUFCMA}^{A}_{\mathcal{MA}} \Rightarrow \text{true}\right] \tag{1}$$

Explain, in words, the difference between SUF-CMA and UF-CMA. We saw in class that a message authentication scheme based on a secure PRF is secure in the sense of UF-CMA. Does the argument extend to SUF-CMA? Explain why or why not.

2. 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 $A_{\mathcal{MA}}$ such that

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

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

main G_0, $\boxed{G_1}$

$K_1 \xleftarrow{\$} \mathcal{K}_e$; $K_2 \xleftarrow{\$} \mathcal{K}_m$; $b \xleftarrow{\$} \{0,1\}$; $S \leftarrow \emptyset$
$b' \xleftarrow{\$} A^{\mathbf{LR},\mathbf{Dec}}$
Return $(b = b')$

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

Figure 2: Game G_1 includes the boxed code and game G_0 does not.

Your proof should use a game sequence that includes the games G_0, G_1 of Fig. 2.

A Generalized birthday lemma

Let N, r be positive integers and let S be a set of size N. Suppose we pick $y_1, \ldots, y_r$ at random from S and also pick $z_1, \ldots, z_r$ at random from S. Let $D(N,r)$ be the probability that there exist i, j such that $y_i = z_j$.

Lemma A.1 Let N, r be positive integers. Then

$$D(N,r) \;\geq\; \frac{C(N,2r)}{2} \; .$$
