Quiz 2 Solutions

Problem 1 [40 points] If A, B are bit-strings of equal length then we let $A \vee B$ denote their bitwise OR. (For example, $10110 \vee 01101 = 11111$.) Let algorithm $\mathcal{K}$ return a random 128-bit string. Let $\mathcal{E}$ be the following encryption algorithm that takes input a message $M = M[1] \cdots M[m]$ consisting 128-bit blocks:

Alg $\mathcal{E}_K(M)$
$C[0] \xleftarrow{\$} \{0,1\}^{128}$
For $i = 1, \ldots, m$ do
$C[i] \leftarrow \mathsf{AES}_K(C[i-1] \vee M[i])$
Return C

1. **[10 points]** Specify a decryption algorithm $\mathcal{D}$ such that $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is a symmetric encryption scheme with correct decryption.

This turns out not to be true. Everyone will get full credit. Sorry about that.

2. **[30 points]** Show that this scheme is insecure by presenting a practical adversary A such that $\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE}}(A)$ is high. Say what is the advantage achieved by your adversary, what is its running time, and how many oracle queries it makes. The number of points you get depends on these quantities.

adversary A
$C_1[0]C_1[1] \xleftarrow{\$} \text{LR}(1^{128}, 1^{128})$
$C_2[0]C_2[1] \xleftarrow{\$} \text{LR}(0^{128}, 1^{128})$
if $C_1[1] = C_2[1]$ **then return** 1 **else return** 0

In either game we have

$$C_1[1] = \mathsf{AES}_K(C_1[0] \vee 1^{128}) = \mathsf{AES}_K(1^{128}).$$

Now suppose we are playing game $\text{Left}_{\mathcal{SE}}$, so that $C_2[0]C_2[1] \xleftarrow{\$} \mathcal{E}_K(0^{128})$. Then

$$C_2[1] = \mathsf{AES}_K(C_2[0] \vee 0^{128}) = \mathsf{AES}_K(C_2[0])\ .$$

Since AES_K is a permutation, we will have $C_1[1] = C_2[1]$ iff $C_2[0] = 1^{128}$. The probability of the latter is 2^{-128} since $C_2[0]$ is chosen at random. Thus

$$\Pr\left[\text{Left}^A_{\mathcal{SE}} \Rightarrow 1\right] = 2^{-128} .$$

Suppose we are playing game $\text{Right}_{\mathcal{SE}}$, so that $C_2[0]C_2[1] \xleftarrow{\$} \mathcal{E}_K(1^{128})$. Then

$$C_2[1] = \mathsf{AES}_K(C_2[0] \vee 1^{128}) = \mathsf{AES}_K(1^{128}) .$$

So we have $C_2[1] = C_1[1]$ and thus

$$\Pr\left[\text{Right}^A_{\mathcal{SE}} \Rightarrow 1\right] = 1 .$$

So

$$\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{SE},A} \geq 1 - 2^{-128} .$$

A makes 2 oracle queries and its running time is very small.

Problem 2 [30 points] Let E: $\{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a secure block cipher with $n \geq 128$. Let the family of functions H: $\{0,1\}^n \times \{0,1\}^{2n} \to \{0,1\}^n$ be defined as follows:

Alg $H_K(M)$
$L \leftarrow K$
For $i = 1, 2$ do
  $X \leftarrow E_L(M[i])$; $L \leftarrow X \oplus M[i]$
Return X

Above $M[1]$ denote the first n bits of M and $M[2]$ the next.

Show that H is not collision resistant by presenting a practical adversary A such that

$$\mathbf{Adv}^{\text{cr}}_H(A) = 1.$$

Note that the running time of the birthday attack is too large for it to be considered practical.

adversary A
  $a_1 \leftarrow 0^n$; $b_1 \leftarrow 0^n$; $a_2 \leftarrow 1^n$
  $L_1 \leftarrow E_K(a_1) \oplus a_1$; $L_2 \leftarrow E_K(a_2) \oplus a_2$
  $X \leftarrow E_{L_1}(b_1)$; $b_2 \leftarrow E^{-1}_{L_2}(X)$
  return $a_1 \,\|\, b_1, a_2 \,\|\, b_2$

This adversary is very practical, using only four E or E^{-1} computations. We claim that the $a_1 \,\|\, b_1, a_2 \,\|\, b_2$ it returns is a collision for H_K, which means that $\mathbf{Adv}^{\mathrm{cr}}_H(A) = 1$. The claim is true because

$$\begin{aligned} H_K(a_1 \,\|\, b_1) &= E_{L_1}(b_1) = X \\ H_K(a_2 \,\|\, b_2) &= E_{L_2}(b_2) = E_{L_2}(E_{L_2}^{-1}(X)) = X \end{aligned}$$

and also a_1, a_2 being different implies $a_1 \,\|\, b_1 \neq a_2 \,\|\, b_2$.

Problem 3 [30 points] Let E: $\{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a secure block cipher with $n \geq 128$. Let $\mathcal{K}$ pick K at random form $\{0,1\}^k$ and L at random from $\{0,1\}^n$ and return $K \,\|\, L$ as the key. Let $\mathcal{MA} = (\mathcal{K}, \mathcal{T}, \mathcal{V})$ be the message authentication scheme whose tagging and verifying algorithms are as follows:

$\underline{\textbf{Alg } \mathcal{T}_{K \,\|\, L}(M)}$	$\underline{\textbf{Alg } \mathcal{V}_{K \,\|\, L}(M,T)}$
$m \leftarrow \lvert M \rvert / n$	If $(\mathcal{T}_{K \,\|\, L}(M) = T)$
$C[0] \leftarrow 0^n$	then return 1
For $i = 1, \ldots, m$ do	Else return 0
$\quad C[i] \leftarrow E_K(C[i-1] \oplus M[i])$	
$T \leftarrow C[m] \oplus L$	
Return T	

Above $|M|$ denote the length of M which is assumed to be a positive multiple of n, and $M[i]$ is the i-th n-bit block of M.

Show that $\mathcal{MA}$ is not UF-CMA secure by presenting a practical adversary A such that

$$\mathbf{Adv}^{\text{uf-cma}}_{\mathcal{MA}}(A) = 1.$$

Full credit requires a (correct) adversary making 3 or less **Tag** queries and 1 **Verify** query.

Adversary $A(K)$
$x_1 \leftarrow 0^n$
$x_2 \leftarrow 1^n$
$y_1 \leftarrow \mathbf{Tag}(x_1)$
$y_2 \leftarrow \mathbf{Tag}(x_2)$
$y \leftarrow \mathbf{Tag}(y_1 \oplus y_2)$
return $(x_1 \,\|\, y_2, y)$

We have

$$\begin{aligned} y_1 &= E_K(x_1) \oplus L \\ y_2 &= E_K(x_2) \oplus L \end{aligned}$$

$$\begin{aligned} y_1 \oplus y_2 &= E_K(x_1) \oplus E_K(x_2) \\ y &= E_K(E_K(x_1) \oplus E_K(x_2)) \oplus L \\ &= \mathcal{T}_K(x_1 \parallel E_K(x_2)) \\ &= \mathcal{T}_K(x_1 \parallel y_2)) \end{aligned}$$

So $\mathbf{Adv}^{\text{uf-cma}}_{\mathcal{MA}}(A) = 1$.
