CC5301: Introducción a la Criptografía Moderna, Otoño 2012 Prof. A. Hevia
Tarea 2 8 de Mayo 2012
Viernes 18 de Mayo 2012, 23:59hrs.

Tarea 2

Instrucciones:

- No se tolerarán copias o cualquier otro comportamiento de deshonestidad académica. En particular, obtener y utilizar soluciones de las preguntas desde Internet (si existiesen) se considerará copia.
- Está tarea se puede discutir en grupos de a lo más dos personas. Sin embargo, no se deben tomar notas durante la discusión, y luego de ella cada miembro del grupo debe entregar su tarea separadamente, escrita y redactada en forma individual, indicando explícitamente el nombre de la persona con la cual se discutió. El no cumplimiento de estas condiciones se considerará copia.
- La tarea debe entregarse en forma digital (formato PDF). Se recomienda utilizar LaTeX. Excepcionalmente se aceptarán tareas que hayan sido escritas a mano y luego digitalizadas como archivos JPG, pero sólo si la presentación es pulcra y limpia.
- **Importante:** Dedique tiempo a escribir su solución, no lo deje para el último minuto. Su nota depende no sólo de la correctitud de su respuesta, si no de la claridad y presentación de su solución. Una solución poco clara, mal o pobremente escrita, aunque esté correcta es probable que obtenga mala nota.
- **Fecha de Entrega:** Viernes 18 de Mayo 2012, 23:59hrs.. La entrega debe hacerse vía u-cursos. Cualquier pregunta hacerla en el foro del curso.

Problema 1 [Total: 40 puntos]

Sean n, b enteros positivos fijos y sea $h\colon \{0,1\}^{n+b} \to \{0,1\}^n$ una función de compresión resistente a la colisión. En clases vimos la transformación Merkle-Damgärd (MD) para producir funciones de hash resistentes a la colisión cuando el mensaje es múltimo de b bits, esto es, $D = (\{0,1\}^b)^*$. Es fácil ver que la misma demostración de seguridad puede extenderse fácilmente para el dominio más general $D = \{0,1\}^*$ como sigue. Primero, se hace *padding* sobre el mensaje con suficientes 0's: esto es, dado $M' \in \{0,1\}^*$, agregar $s > 0$ ceros, tal que el largo de $M = M'||0^s$ es múltiplo de b. Luego, se aplica la construcción MD vista en clases usando $\ell = |M|$ el largo en bits en vez de $m = ||M||_b$.

Indique si las siguientes variantes de la transformación (MD) para $D = \{0,1\}^*$ descrita producen funciones de hash resistentes a la colisión o no. Si lo es, entregue una demostración; si no, muestre un ataque. (La notación es la usada en clases, excepto que $\ell = |M|$ es el largo en bits de M y $m = ||M||_b$.)

(a). Modificar la construcción para no agregar el último bloque con el largo al final, esto es, retornar $H_K(M) = V[m]$.

(b). Modificar la construcción para en vez de retornar $H_K(M) = V[m+1] = h_K(\langle\ell\rangle||V[m])$ ahora retorne $H_K(M) = \langle\ell\rangle||V[m]$.

(c). En vez de usar $V[0] = 0^n$ en la primera iteracion de h_K, usar $V[0] \xleftarrow{R} \{0,1\}^n$ y luego entregar $H_K(M) = V[0] \,||\, h_K(\langle\ell\rangle||V[m])$ como resultado. (Notar que esta transformación produce una función $H\colon \{0,1\}^{\leq 2^b} \to \{0,1\}^{2n}$).

(d). Omitir el uso de 0^n como vector de inicialización y simplemente empezar a procesar M. Esto es, en vez de usar $V[0] = 0^n$ en la primera iteracion de h_K, usar $V[0] \leftarrow M[1]$, luego iterar con $V[i] \leftarrow h_K(M[i+1]||V[i])$ para $i = 1, \ldots, m$ (donde $M[m+1] = \langle\ell\rangle$), y entregar $H_K(M) = V[m]$ como resultado.

(e). En vez de usar $V[0] = 0^n$ en la primera iteración de h_K, usar $V[0] = \langle\ell\rangle$, y luego retornar $H_K(M) = V[m]$.

Problema 2 [Total: 40 puntos]

En esta pregunta veremos la manera de obtener un esquema de encriptación simétrico seguro en el sentido `IND-CCA`. Sea $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ un esquema de encriptación simétrico seguro en el sentido `IND-CPA`, y sea $\mathcal{MA} = (\mathcal{K}', MAC, VF)$ un esquema de autentificación de mensajes seguro en el sentido `SUF-CMA` (*Strong Unforgeability under chosen-message attacks*). Considere el esquema de encriptación $\overline{\mathcal{SE}} = (\overline{\mathcal{K}}, \overline{\mathcal{E}}, \overline{\mathcal{D}})$ definido como

- Algoritmo $\overline{\mathcal{K}}(\cdot)$ = "$K_1 \xleftarrow{R} \mathcal{K}$, $K_2 \xleftarrow{R} \mathcal{K}'$, $K \leftarrow (K_1, K_2)$, return K."
- Algoritmo $\overline{\mathcal{E}}(K, M)$ = "$C' \xleftarrow{R} \mathcal{E}_{K_1}(M)$, $\tau = MAC_{K_2}(C')$, $C \leftarrow (C', \tau)$, return C."
- Algoritmo $\overline{\mathcal{D}}(K, C)$ = "Interpreta C como (C', τ). Si $VF_{K_2}(C', \tau) = 1$ entonces $M \leftarrow \mathcal{D}_{K_1}(C')$, return M; Sino, return $\perp$."

esto es, los textos cifrados son iguales a los generados por $\mathcal{SE}$ excepto que tienen adjunto además un tag (generado por $\mathcal{MA}$) para verificar la "autenticidad" del texto cifrado.

(a). [30 puntos] Demuestre vía una reducción que, bajo los supuestos hechos antes, $\overline{\mathcal{SE}}$ es `IND-CCA` seguro.

(b). [10 puntos] Demuestre que la condición `Strong` se necesita, esto es, muestre un ejemplo de un esquema de autentificación $\mathcal{MA}^*$ del tipo `UF-CMA` seguro que, al ser usado para construir $\overline{\mathcal{SE}}$ causa que este último NO sea `IND-CCA` seguro.

Problema 3 [Total: 20 puntos]

Sea $E\colon \{0,1\}^k \times B \to B$ un cifrador de bloque, donde $B = \{0,1\}^n$ y $n > 32$. Cada mensaje $M \in B^*$ es una secuencia de m bloques de ℓ bits: $M = M[1]\cdots M[m]$ donde $\ell = n - 32$. Denotaremos por $\langle i \rangle$ a la representación del índice i como entero binario de 32 bits. Sea $\mathcal{MA} = (\mathcal{K}, \mathcal{T}, \mathcal{V})$ el esquema de autentificación de mensajes donde $\mathcal{K}$ entrega una clave uniformemente distribuída, $\mathcal{V}$ es el algoritmo de verificación canónica, y $\mathcal{T}_K$ opera como sigue: dado el mensaje $M = M[1]\ldots M[m]$, primero escoge $r \xleftarrow{R} B$, luego calcula

$$t \leftarrow E_K(r) \oplus E_K(\langle 1 \rangle || M[1]) \oplus \cdots \oplus E_K(\langle m \rangle || M[m])$$

y retorna como etiqueta (r, t). Demuestre que este esquema no es seguro, esto es, existe un adversario razonable cuya ventaja UF-CMA es cercana a 1.

Suerte!