CC51D, Seguridad de Datos **15 de Septiembre, 2006**

Solución Control 1

Profesor: Alejandro Hevia Semestre Primavera 2006

PROBLEMA 1: (Total 10 puntos)

Demuestre que, para toda clave $K = (K_1||K_2)$ (donde $K_1, K_2 \in \{0,1\}^{56}$) y todo mensaje $M \in \{0,1\}^{64}$, se tiene que $\texttt{3DES}_{\overline{K_1||K_2}}(\overline{M}) = \overline{\texttt{3DES}_{K_1||K_2}(M)}$.

SOLUCIÓN:

Primero que nada, vimos en clase la propiedad de "complementaridad"de DES:

$$\overline{\texttt{DES}_K(M)} \;=\; \texttt{DES}_{\overline{K}}(\overline{M})$$

o equivalentemente que

$$\texttt{DES}_K(M) \;=\; \overline{\texttt{DES}_{\overline{K}}(\overline{M})}\,. \tag{1}$$

Antes de demostrar lo pedido, nos será útil probar que la misma relación se cumple con la función inversa de DES esto es:

$$\texttt{DES}_K^{-1}(M) \;=\; \overline{\texttt{DES}_{\overline{K}}^{-1}(\overline{M})}\,. \tag{2}$$

La demostración es simple. Dado $M \in \{0,1\}^{64}$ y $K \in \{0,1\}^{56}$ arbitrarios, calculemos $\texttt{DES}_K\left(\overline{\texttt{DES}_{\overline{K}}^{-1}(\overline{M})}\right)$. Usando (1),

$$\texttt{DES}_K\left(\overline{\texttt{DES}_{\overline{K}}^{-1}(\overline{M})}\right) \;=\; \overline{\texttt{DES}_{\overline{K}}(\texttt{DES}_{\overline{K}}^{-1}(\overline{M}))} \;=\; \overline{\overline{M}} \;=\; M\,.$$

y aplicando $\texttt{DES}_K^{-1}(\cdot)$ a ambos lados de la equación obtenemos (2).

Ahora bien, para demostrar el resultado pedido, dado $M \in \{0,1\}^{64}$ y $K_1, K_2 \in \{0,1\}^{56}$ arbitrarios, hacemos lo siguiente:

$$\begin{aligned}
\texttt{3DES}_{\overline{K_1||K_2}}(\overline{M}) &= \texttt{DES}_{\overline{K_2}}(\texttt{DES}_{\overline{K_1}}^{-1}(\texttt{DES}_{\overline{K_2}}(\overline{M})))\\
&= \texttt{DES}_{\overline{K_2}}(\texttt{DES}_{\overline{K_1}}^{-1}(\overline{\texttt{DES}_{K_2}(M)}))\\
&= \texttt{DES}_{\overline{K_2}}(\overline{\texttt{DES}_{K_1}^{-1}(\texttt{DES}_{K_2}(M))})\\
&= \overline{\texttt{DES}_{K_2}(\texttt{DES}_{K_1}^{-1}(\texttt{DES}_{K_2}(M)))}\\
&= \overline{\texttt{3DES}_{K_1||K_2}(M)}
\end{aligned}$$

donde cada igualdad se obtiene aplicando (1) o bien (2).

(Nota: debido a un error de tipeo, en las transparencias de clases la (1) aparecía en forma incorrecta. Sólo se considerará esta pregunta como bonus adicional *de 5 pts. a quienes la hayan resuelto correctamente.)*

PROBLEMA 2: (Total 20 puntos) Un banco usa el siguiente método para permitir a un cliente Beatriz identificarse a un cajero automático. El banco inicialmente le entrega a Beatriz un número secreto p de 6 digitos, escogido al azar. (A este número se le llama "PIN"). El banco también guarda este número en forma segura en su servidor. Cuando Beatriz ingresa su tarjeta bancaria en el cajero automático, entonces:

1. El cajero envía el mensaje "`Beatriz`" al banco.

2. El banco escoge al azar un string C de 128 bits (denominado el *desafío* o *challenge*) y lo envía al cajero automático.

3. El cajero a continuación solicita a Beatriz su PIN. Una vez que Beatriz ingresa `p`, el cajero calcula $X = \texttt{SHA1}(C||\texttt{p})$ el cual envía al banco.

4. El banco recibe X y recupera `p` de sus registros en el servidor. Luego, el banco acepta a Beatriz como usuario válido si y sólo si $\texttt{SHA1}(C, \texttt{p}) == X$, en cuyo caso le envía al cajero el mensaje "`Beatriz-ok`".

Suponga que el canal de comunicación entre el cajero y el banco es monitoreado por un atacante que puede obtener toda la información comunicada entre el banco y el cajero. Discuta la seguridad del sistema. En particular, describa un objetivo de seguridad, haga una evaluación de amenazas, y un análisis de seguridad. Sea explícito con todos sus supuestos.

SOLUCIÓN:

El análisis debería incluir los siguientes puntos:

1. Objetivo de seguridad: autentificar a un usuario válido (Beatriz), Opcional: explicar qué es un usuario válido y/o qué es autentificar.

2. Evaluación de las amenazas: adversario básico puede leer todos los mensajes pero no modificar mensajes existentes ni injectar nuevos; adversario debe ser "razonable", esto es, su tiempo de ejecución y número de mensajes que puede acceder no es muy alto (por ej. a lo más 2^{60} operaciones aprox.) Opcional: Un adversario sofisticado sería uno "razonable"que además puede modificar/injectar mensajes.

3. El sistema es inseguro ante adversarios básicos (y por ende ante adversarios sofisticados también) puesto que un adversario A que ve el parámetro C puede deducir el PIN `p` en a lo más $10^6 = 2^{6*\log_2(10)} \approx 2^{20}$ operaciones de cálculo de SHA-1, y luego conectarse como un usuario válido. Opcional: Un adversario sofisticado puede quebrar el objetivo de seguridad simplemente enviando el mensaje "`Beatriz-ok`" al cajero después de ingresar cualquier PIN.

PROBLEMA 3: (Total 20 puntos) Sea $\mathcal{AE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ un sistema de encriptación. Suponga que le dan un adversario B que puede extraer el i-ésimo bit del texto plano teniendo sólo el texto cifrado. Esto es, para toda clave $K \in \{0,1\}^k$ y todo texto plano $M \in \{0,1\}^n$, donde $M = M_1, \ldots, M_n$, dado un texto cifrado $C = \mathcal{E}_K(M)$, $B(C)$ entrega como output el bit M_i para un indice i al azar entre 1 y n. Demuestre como construir un adversario A que quiebra el sistema de encriptacion propuesto, en el sentido que viola la propiedad `IND-ATPE`. Esto es, muestre un adversario razonable A que tenga $\texttt{Ventaja-IND-ATPE}(\mathcal{AE}, A)$ cercana o igual a 1. Indique claramente el (pseudo)código de A (qué pasos realiza) y el número de preguntas hechas al oráculo.

SOLUCIÓN:

El siguiente adversario A tiene $\texttt{Ventaja-IND-ATPE}(\mathcal{AE}, A) = 1$.

Adversario A: `// A tiene acceso a oráculo IzqDer`
  Sea $M^{(0)} \leftarrow 0^n$, $M^{(1)} \leftarrow 1^n$

Enviar $(M^{(0)}M^{(1)})$ al oráculo IzqDer; obtiene C como respuesta.
Si $B(C) = 1$ output $g = 1$, si no, ouput $g = 0$.

Claramente, no importa cúal bit i del texto plano el adversario puede recuperar, adversario B entrega 1 si y sólo si el mensaje $M^{(1)}$ fue el encriptado. Por ende, no importa el valor del bit b escogido en el experimento, B siempre gana, y entrega $g = b$. Así,

$$\begin{aligned} \texttt{Ventaja-IND-ATPE}(\mathcal{AE}, A) &= \Pr[\, A \text{ gana experimento}\,] \\ &= |2 \cdot \Pr[\, g = b\,] - 1| \\ &= |2 \cdot 1 - 1| \;=\; 1\,. \end{aligned}$$

Este adversario realiza sólo 1 pregunta al oráculo.

Problema 4: (Total 30 puntos) Sea K una clave para DES de 56 bits y L una clave auxiliar de 64 bits. Para todo texto plano M de 64 bits,

$$\texttt{DESY}(K||L, M) = \texttt{DES}(K, L \oplus M)\,.$$

Esto define una familia de funciones $\texttt{DESY} : \{0,1\}^{120} \times \{0,1\}^{64} \to \{0,1\}^{64}$.

1. (10 puntos) Demuestre que DESY es un cifrador de bloque.
2. (20 puntos) Sea $(M_1, C_1), (M_2, C_2)$ dos pares texto plano y texto cifrado obtenidos usando DESY bajo una clave aleatoria $K||L$ de 120 bits. Muestre un ataque que, dado $(M_1, C_1), (M_2, C_2)$ se puede recuperar la clave $K||L$ correspondiente usando a lo más 2^{57} operaciones de DES o $\texttt{DES}^{-1}$.

Solución:

1. Para demostrar que DESY es un cifrador de bloque basta demostrar que para cada clave $(K||L) \in \{0,1\}^{120}$, la función de DESY es biyectiva. En rigor, esto significa demostrar que, para toda clave $(K||L)$, $\texttt{DESY}(K||L, \cdot)$ es una función bien definida para todo $M \in \{0,1\}^{64}$ (o sea, que existe un y sólo un valor de $\texttt{DESY}(K||L, M)$) y que tiene una función inversa bien definida para todo el dominio. Como la dificultad de esta parte estaba en lo último, se evaluó sólo esta última parte.

   Claramente, para toda clave $(K||L) \in \{0,1\}^{120}$, $\texttt{DESY}(K||L, \cdot)$ es una función bien definida para todo $M \in \{0,1\}^{64}$ pues DES está bien definida para todo $M \in \{0,1\}^{64}$.

   La función inversa de DESY es:

   $$\texttt{DESY}^{-1}(K||L, C) = \texttt{DES}^{-1}(K, M) \oplus L\,.$$

   puesto que $\texttt{DESY}^{-1}(K||L, (\texttt{DESY}(K||L, M)) = \texttt{DES}^{-1}(K, \texttt{DES}(K, L \oplus M)) \oplus L = L \oplus M \oplus L = M$.

2. Dado dos pares $(M_1, C_1), (M_2, C_2)$ consideremos el siguiente algoritmo.

   Algoritmo $\texttt{AtaqueADESY}((M_1, C_1), (M_2, C_2))$:
   Para cada clave $\kappa \in \{0,1\}^{56}$ hacer:
   Calcular $X \leftarrow \texttt{DES}^{-1}(\kappa, C_1) \oplus M_1$
   Poner (κ, X) en una tabla de hash indexada por X.
   Para cada clave $\theta \in \{0,1\}^{56}$ hacer:
   Calcular $Y \leftarrow \texttt{DES}^{-1}(\theta, C_2) \oplus M_2$
   Testear si existe un registro (κ, Y) en la tabla de hash bajo el índice Y.
   Si es así y $\kappa == \theta$, output $(\kappa||Y)$ y terminar, si no, seguir.
   Si no encontró nada, output "Pares $(M_1, C_1), (M_2, C_2)$ no son usan la misma clave".

Análisis: Notemos que si A entrega una clave $(\kappa||Y)$ esta clave satisface $Y = \texttt{DES}^{-1}(\kappa, C_1) \oplus M_1$, o equivalentemente que $\texttt{DES}(\kappa, Y \oplus M_1) = C_1$, y además que $Y = \texttt{DES}^{-1}(\theta, C_2) \oplus M_2$, o equivalentemente que $\texttt{DES}(\kappa, Y \oplus M_2) = C_2$. Como $\kappa = \theta$ tenemos que $K = (\kappa||Y)$ es para todo los efectos prácticos la clave usada en la encriptación de M_1 y M_2.[1]

El número de operaciones $\texttt{AES}^{-1}$ requeridas es 2^{56} para el primer loop de A, y (a lo más) 2^{56} para el segundo loop. Esto es, un total de $2^{56} + 2^{56} = 2^{57}$ operaciones $\texttt{AES}^{-1}$.

PROBLEMA 5: (Total 20 puntos) Considere la siguiente función de hash $H : \{0,1\}^{192} \to \{0,1\}^{128}$ definida de la siguiente manera. Sea K un string de 64 bits, escogido al azar al inicio de la operación del sistema y comunicado a todo el mundo (esto es, K es público). Definimos la función de hash H como sigue:

Funcion $H(M)$: // $|M| = 192$
Interpreta M como $A||B$ donde $|A| = 64$ y $|B| = 128$
$y \leftarrow \texttt{AES}_{K||A}(B)$ // Calcula y como AES con clave de 128 bits $K||A$ sobre input B
Retorna y

Muestre que H no es resistente a la colisión, presentando un adversario razonable A que encuentra una colisión con alta probabilidad. Indique claramente el tiempo de ejecución de A en términos de el número de operaciones de AES o $\texttt{AES}^{-1}$ necesarias, y la probabilidad que el adversario encuentre la colisión. (Mientras mejor el ataque, más puntos obtendrá en la pregunta).

SOLUCIÓN:

El siguiente adversario A encuentra una colisión:

Adversario A:
Elige $M_0 = A_0||B_0$ donde $A_0 \in \{0,1\}^{64}$ y $B_0 \in \{0,1\}^{128}$ son strings arbitrarios.
Calcula $C \leftarrow H(M_0)$
Elige $A_1 \in \{0,1\}^{64}$ en forma arbitraria pero satisfaciendo $A_1 \neq A_0$.
Calcula $B_1 \leftarrow \texttt{AES}^{-1}_{K||A_1}(C)$
$M_1 \leftarrow A_1||B_1$
Retorna (M_0, M_1)

Demostremos que (M_0, M_1) es una colisión bajo $H(\cdot)$. Claramente, $C = H(M_0)$. Además

$$H(M_1) \;=\; \texttt{AES}_{K||A_1}(B_1) \;=\; \texttt{AES}_{K||A_1}(\texttt{AES}^{-1}_{K||A_1}(C)) \;=\; C$$

Como $A_1 \neq A_0$ por construcción, tenemos que $M_0 \neq M_1$ y el par (M_0, M_1) es una colisión bajo $H(\cdot)$.

Adversario A encuentra colisiones con probabilidad 1 usando una operación de cálculo de AES y otra de cálculo de $\texttt{AES}^{-1}$.

[1] Pudiera existir *dos* claves $Z = (K||L)$ y $Z' = (K'||L')$ que satisfagan $C_1 = \texttt{DESY}(Z, M_1) = \texttt{DESY}(Z', M_1)$ y $C_2 = \texttt{DESY}(Z, M_2) = \texttt{DESY}(Z', M_2)$ pero sean distintas $Z \neq Z'$. Pero, para nuestros efectos, la clave obtenida "funciona"por lo que la consideramos válida. En un ataque real, deberíamos usar más pares texto plano/texto cifrado para aumentar la certeza de que la clave encontrada es la correcta.