Control 1

Profesor: Alejandro Hevia

Semestre Primavera 2006

Con apuntes estrictamente personales.

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 $3DES_{\overline{K_1 || K_2}}(\overline{M}) = 3DES_{K_1 || K_2}(M)$.

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 dígitos, 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 $X = \text{SHA1}(C || p)$ 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 $\text{SHA1}(C, p) == X$, 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.

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 $M = M_1, \dots, M_n$, dado un texto cifrado $C = \mathcal{E}_K(M)$, $B(C)$ entrega como output el bit M_i para un índice i al azar entre 1 y n . Demuestre como construir un adversario A que quiebra el sistema de encriptación propuesto, en el sentido que viola la propiedad IND-ATPE. Esto es, muestre un adversario razonable A que tenga $\text{Ventaja-IND-ATPE}(\mathcal{AE}, A)$ cercana o igual a 1. Indique claramente el (pseudo)código de A (qué pasos realiza) y el número de preguntas hechas al oráculo.

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,

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

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

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 DES^{-1} .

PROBLEMA 5: (Total 20 puntos) Considere la siguiente función de hash $H : \{0, 1\}^{192} \rightarrow \{0, 1\}^{128}$ 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  $|B| = 128$ 
   $y \leftarrow \text{AES}_{K||A}(B)$  // 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 AES^{-1} necesarias, y la probabilidad que el adversario encuentre la colisión. (Mientras mejor el ataque, más puntos obtendrá en la pregunta).