CC5301: Introducción a la Criptografía Moderna, Otoño 2012 Prof. A. Hevia
Tarea 1 9 de Abril 2012
Entrega: Lunes 23 de Abril 2012, 23:59hrs.

Tarea 1

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 es individual pero se puede discutir en grupos de a lo más dos personas. Sin embargo, no se deben tomar notas durante la discusión, y terminada ella cada miembro del grupo debe entregar su tarea separadamente, escrita y redactada en forma individual. El no cumplimiento de esta condición se considerará copia.
- La tarea debe entregarse en forma digital (formato PDF) preferiblemente en LaTeX.
- **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:** Lunes 23 de Abril 2012, 23:59hrs.. La entrega debe hacerse vía u-cursos. Cualquier pregunta hacerla en el foro del curso.

Problema 1 [25 puntos]

En un intento para prevenir el ataque de Kasiski sobre el cifrador Vigenére, se propone la siguiente modificación. Dado el largo de la clave t del cifrador, el texto plano es dividido en bloques de tamaño t. En el cifrador de Vigenére original, el i-ésimo carácter de cada uno de estos bloques es encriptado simplemente sumándolo al i-ésimo carácter de la clave. Si denotamos $k_1, \ldots, k_t$ la clave, lo anterior significa que el i-ésimo carácter de cada bloque es encriptado sumándole k_i al mismo, módulo 26. La modificación propuesta es encriptar ahora el i-ésimo carácter en el j-ésimo bloque sumándole $k_i + j$ módulo 26.

- [5 puntos] Muestra cómo desencriptar.
- [10 puntos] Describa el efecto de la modificación anterior sobre el test de Kasiski.
- [10 puntos] Describa una manera alternativa de determinar el largo de la clave.

Problema 2 [30 puntos]

En este problema estudiamos como vencer el límite de Shannon respecto a que el espacio de claves debe ser igual o mayor que el espacio de mensajes. Supongamos que relajamos la definición de un esquema de encriptación simétrico $(\mathcal{G}, \mathcal{E}, \mathcal{D})$ sobre un espacio de mensajes $\mathcal{M}$ como sigue. Para todo $m \in \mathcal{M}$, la probabilidad que $\mathcal{D}_K(\mathcal{E}_K(m)) = m$ es al menos $\epsilon = 2^t$. (Observar que esta probabilidad está tomada sobre la elección aleatoria de K así como cualquier aleatoriedad usada por los algoritmos de encriptación $\mathcal{E}$ y desencriptación $\mathcal{D}$.) Demuestre que se tiene confidencialidad perfecta si $|\mathcal{K}| \leq |\mathcal{M}|$ cuando $t \geq 1$. De una cota inferior para el tamaño de $\mathcal{K}$.

Problema 3 [25 puntos]

Sea $F\colon \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$ sea una familia de funciones y sea $r \geq 1$ un entero. Un cifrador de Feistel de r rondas asociado a F es la familia de permutaciones $F^{(r)}\colon \{0,1\}^{rk} \times \{0,1\}^{2\ell} \to \{0,1\}^{2\ell}$ definido como sigue: para cualquier $K_1, \ldots, K_r \in \{0,1\}^k$ y entrada $x \in \{0,1\}^{2\ell}$:

Function $F^{(r)}(K1||K_2||\ldots||K_r, x)$
  Parsear x como $L_0||R_0$ con $|L_0| = |R_0| = \ell$
  For $i = 1, \ldots, r$ do
    $L_i \leftarrow R_{i-1}$; $R_i \leftarrow F(K_i, R_{i-1}) \oplus L_{i-1}$
  Return $L_r||R_r$

Demostrar que existe un adversario PRF A quien, haciendo a lo más dos preguntas a su oráculo y corriendo en tiempo cercano al que toma calcular dos computaciones de F, tal que $\mathbf{Adv}^{prf}_F(A) \geq 1 - 2^{-\ell}$.

Problema 3 [20 puntos]

Consideremos la siguiente definición alternativa de PRF. Es un juego donde se tira una moneda y, si es cara el adversario es ubicado en el juego Real, y si es sello es ubicado en el juego Aleatorio; el adversario "gana" si puede adivinar el valor de la moneda. En este problema queremos demostrar que tal definición es equivalente a la definición de PRF dada en clases.

Sea $F\colon \texttt{Claves}(F) \times \texttt{Dom}(F) \to \texttt{Rec}(F)$ una familia de funciones y sea A un adversario que toma oráculo.

Juego $\texttt{PRFcg}_F^A$:

PROC Inicializar
  $K \xleftarrow{\$} \{0,1\}^k$; $b \xleftarrow{\$} \{0,1\}$

PROC $\mathbf{Fn}_1(x)$
  Return $F_K(x)$

PROC $\mathbf{Fn}_0(x)$
  $T[x] \xleftarrow{\$} \texttt{Rec}(F)$; Return $T[x]$

PROC `GuessWorld`
  if $b = 1$ then $g \leftarrow A^{\mathbf{Fn}_1(\cdot)}$;
  else $g \leftarrow A^{\mathbf{Fn}_0(\cdot)}$;
  if $g = b$ then return 1 else return 0

Figure 1: Juego $\texttt{PRFcg}_F^A$ para el problema 5.

Considere el juego $\texttt{PRFcg}_F^A$ mostrado en la Figura 1. Definimos $\texttt{PRFcg}_F^A \Rightarrow 1$ como el evento donde el procedimiento `GuessWorld` retorna 1, y la ventaja `PRF-CG` de A como $\mathbf{Adv}_F^{\text{prf-cg}}(A) \stackrel{\text{def}}{=} |2 \cdot Pr\left[\texttt{PRFcg}_F^A \Rightarrow 1\right] - 1|$.

Demuestre que para toda familia F y todo adversario A se tiene que $\mathbf{Adv}_F^{\text{prf}}(A) = \mathbf{Adv}_F^{\text{prf-cg}}(A)$.

Suerte!