PONTIFICIA UNIVERSIDAD CATOLICA DE CHILE
ESCUELA DE INGENIERIA
DEPARTAMENTO DE CIENCIA DE LA COMPUTACION

Criptografía y Seguridad Computacional - IIC3253
Rúbrica Tarea 1

Preguntas

1. En esta pregunta usted deberá obtener una llave utilizada para encriptar mensajes con una variante de OTP bastante mala. Deberá entregar un archivo `Pregunta_1/key.bin` que contenga la llave que se utilizó para encriptar dichos mensajes, además de un notebook que explique el proceso que se siguió para obtener la llave.

   Los mensajes que debe decriptar serán subidos a su repositorio privado a lo más 24 horas después de su creación (ver Configuración Inicial más arriba).

   Corrección. El puntaje de esta pregunta se calcula como $6 \cdot r \cdot (0.7 + 0.3 \cdot d)$, donde r (ratio) es la proporción de caracteres correctos de la llave y d (desarrollo) se calcula de acuerdo a los puntajes que se muestran más abajo. Por ejemplo, si se consigue 48 de los 64 bytes de la llave y d es 0.5, entonces el puntaje de esta pregunta será $6 \cdot 48/64 \cdot (0.7 + 0.3 \cdot 0.5) = 3.825$. Se considerará que la llave tiene 64 bytes aunque en realidad era dos veces una llave de 32 bytes. Si alguien simplemente respondió con 32 bytes, se considerará la proporción de bytes correctos en dicha llave.

   Cálculo del valor d:

   - [0] Entrega un notebook vació o que no aporta información concreta respecto de cómo se obtuvo la llave.
   - [0.5] Entrega un notebook que explica ciertos pasos para conseguir la llave, pero ciertas partes de la llave cuya obtención no es obvia, aparecen sin una explicación.
   - [1] El notebook describe de forma concreta cómo se obtuvieron los caracteres de la llave entregada.

2. Sea $\ell > 0$ un número entero, sea $\mathcal{M}$ el siguiente espacio de mensajes:

$$\mathcal{M} \quad = \quad \{\varepsilon\} \cup \{0,1\} \cup \{0,1\}^2 \cup \{0,1\}^3 \cup \cdots \cup \{0,1\}^\ell,$$

   donde ε es la palabra vacía, y sea $\mathcal{K} = \{0,1\}^{\ell+1}$. Defina un espacio de textos cifrados $\mathcal{C}$ que sea subconjunto de $\{0,1\}^*$, y un esquema criptográfico (Gen, Enc, Dec) sobre $\mathcal{K}$, $\mathcal{M}$ y $\mathcal{C}$ que

sea perfectamente secreto.

Nota: En la definición de (Gen, Enc, Dec) debe suponer que Gen es la distribución uniforme sobre $\mathcal{K}$.

Corrección. Esta pregunta se corrige considerando que se debe diseñar un esquema criptográfico (Gen, Enc, Dec) que sea perfectamente secreto. La asignación de puntaje en esta pregunta es la siguiente.

- [1.5 puntos] Sólo se entrega la definición del esquema esquema criptográfico (Gen, Enc, Dec), la cual incluye las definiciones del espacio de mensajes cifrado $\mathcal{C}$ y las familias de funciones Enc y Dec, y no está completamente correcta.
- [3 puntos] Se entrega una definición correcta del esquema esquema criptográfico (Gen, Enc, Dec), la cual incluye las definiciones del espacio de mensajes cifrado $\mathcal{C}$ y las familias de funciones Enc y Dec.
- [4.5 puntos] Se entrega una definición correcta del esquema criptográfico (Gen, Enc, Dec), la cual incluye las definiciones del espacio de mensajes cifrado $\mathcal{C}$ y las familias de funciones Enc y Dec, y se demuestra formalmente que este esquema es correcto (en el sentido que $Dec_k(Enc_k(m)) = m$).
- [6 puntos] Se entrega una definición correcta del esquema criptográfico (Gen, Enc, Dec), la cual incluye las definiciones del espacio de mensajes cifrado $\mathcal{C}$ y las familias de funciones Enc y Dec, se demuestra formalmente que este esquema es correcto (en el sentido que $Dec_k(Enc_k(m)) = m$), y se demuestra formalmente que este esquema es perfectamente secreto.

3. Considere el juego que define una PRP con una ronda sobre OTP. Demuestre que todo avdersario tiene una probabilidad de ganar de exactamente 1/2.

   Bonus: ¿Es cierto lo anterior si consideramos cualquier protocolo que satisface la propiedad de perfect secrecy? Demuestre o de un contraejemplo.

Corrección. Hay varias formas de demostrar lo que se pide, y por lo tanto la asignación de puntajes sigue un esquema basado en el razonamiento y la capacidad de hacer una demostración correcta y bien escrita.

- [0 puntos] No entrega una demostración o la demostración no tiene una narrativa clara, de lo que está escrito realmente no se puede entender lo que se intentaba hacer.
- [1.5 punto] De lo que se intenta demostrar no se deduce directamente que la probabilidad sea 1/2. Además la demostración no es correcta y/o es difícil de seguir.
- [3 puntos] De lo que se intenta demostrar no se deduce directamente que la probabilidad sea 1/2. La demostración es correcta y se entiende.
- [4.5 puntos] La narrativa de la demostración es correcta y de ella se deduce que la probabilidad es 1/2, pero la demostración es incorrecta y/o difícil de seguir.

- [6 puntos] La narrativa de la demostración es correcta y de ella se deduce que la probabilidad es 1/2. La demostración no se salta pasos y muestra todos los detalles, es fácil de seguir.
- [8 puntos] Se cumple la descripción anterior tanto para el ejercicio como para el bonus.

4. En ayudantía fue demostrado que si una función de hash es resistente a colisiones, entonces esta función debe ser resistente a preimagen. En esta pregunta usted debe demostrar que la implicación inversa no es cierta. Vale decir, suponiendo que existe una función de hash que es resistente a preimagen, demuestre que existe una función de hash (Gen, h) que es resistente a preimagen y no es resistente a colisiones.

   Corrección. La asignación de puntaje en esta pregunta es la siguiente.

   - [1.5 puntos] Sólo se entrega la definición de la función de hash (Gen, h), la cual no está completamente correcta.
   - [3 puntos] Se entrega una definición correcta de la función de hash (Gen, h).
   - [4.5 puntos] Se entrega una definición correcta de la función de hash (Gen, h), y se demuestra que es resistente a preimagen.
   - [6 puntos] Se entrega una definición correcta de la función de (Gen, h), se demuestra que es resistente a preimagen y se demuestra que no es resistente a colisiones.