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 decriptar un mensaje que ha sido encriptado usando OTP, pero cometiendo el error de usar una llave más corta que el mensaje a encriptar.

   Los ayudantes crearán una rama en su repositorio personal llamada *tarea-1*, que contendrá el archivo `/Tarea1/Pregunta1/cipher.txt`. Usted deberá decriptar el contenido de dicho archivo, y dejar un archivo `/Tarea1/Pregunta1/plain.txt` en la rama `main` de su repositorio a modo de solución. Este archivo deberá contener el texto plano original que fue encriptado.

   En el repositorio del curso encontrará un ejemplo del archivo que subirán los ayudantes del curso a su repositorio personal, en `/Tareas/Tarea1/ejemplo_pregunta_1/cipher.txt`. También encontrará el archivo `/Tareas/Tarea1/ejemplo_pregunta_1/plain.txt`, que corresponde al texto plano original, ejemplificando lo que usted tendrá que entregar.

   Corrección. Esta pregunta se corrige considerando cuánto se parece el mensaje entregado al texto que realmente se utilizó al momento de encriptar, y que el mensaje entregado sea efectivamente el resultado de decriptar el archivo `cipher.txt` con una llave de largo menor que el largo del contenido de dicho archivo.

   - [1.5 puntos] Se entrega un texto que resulta de decriptar `cipher.txt` con una llave más corta, y el texto que se entrega tiene características que pueden ser consideradas como estadísticamente relevantes. Sin embargo, el texto entregado no tiene un sentido claro. Por ejemplo, si alguien entrega un archivo que sólo contiene números, letras, espacios y puntuación, pero distribuidos de forma que no hacen sentido, y el archivo efectivamente se obtiene como resultado de decriptar el texto cifrado con una llave más corta.
   - [3 puntos] El texto entregado coincide, byte a byte, al menos en un 30% con el texto plano original.
   - [4.5 puntos] El texto entregado coincide, byte a byte, al menos en un 60% con el texto plano original.
   - [5 puntos] El texto entregado coincide, byte a byte, al menos en un 90% con el texto plano original.

- [5.8 puntos] Se entrega un texto que coincide, byte a byte, al menos en un 95% con el texto utilizado originalmente, pero dicho texto no se puede obtener en base a decriptar el texto cifrado con una llave más corta.
- [6 puntos] Se entrega un texto que coincide, byte a byte, al menos en un 95% con el texto utilizado originalmente, y dicho texto se obtiene en base a decriptar el texto cifrado con una llave más corta.

2. Sean q y n dos números naturales tales que $6 \leq q \leq n$, y sea (Gen, Enc, Dec) un esquema criptográfico definido sobre los espacios $\mathcal{M} = \mathcal{C} = \{0,1\}^n$ y $\mathcal{K} = \{0,1\}^{nq-1}$. En esta pregunta usted debe demostrar que este esquema no es una pseudo-random permutation (PRP) con q rondas. En particular, debe demostrar que el adversario gana el juego que define una PRP con una probabilidad mayor o igual a $\frac{1}{2} + \frac{1}{6}$.

   Corrección. Esta pregunta se corrige considerando que se debe definir la estrategia del adversario que le permite ganar el juego de q rondas que define una PRP con una probabilidad mayor o igual a $\frac{1}{2} + \frac{1}{6}$. La asignación de puntaje en esta pregunta es la siguiente.

   - [1.5 puntos] Sólo se entrega la definición de la estrategia del adversario. Esta estrategía tiene elementos que efectivamente podrían permitir al adversario ganar con una probabilidad significativamente mayor a $\frac{1}{2}$, pero tiene algunos errores.
   - [3 puntos] Se entrega una definición de la estrategia del adversario que está correcta en el sentido de que le permite al adversario ganar el juego con probabilidad mayor o igual a $\frac{1}{2} + \frac{1}{6}$.
   - [4.5 puntos] Se entrega una definición de la estrategia del adversario que está correcta en el sentido de que le permite al adversario ganar el juego con probabilidad mayor o igual a $\frac{1}{2} + \frac{1}{6}$. Además se explica por qué la probabilidad de que el adversario gane el juego es mayor o igual a $\frac{1}{2} + \frac{1}{6}$, pero no se entrega una demostración completa de esta propiedad.
   - [6 puntos] Se entrega una definición de la estrategia del adversario que está correcta en el sentido de que le permite al adversario ganar el juego con probabilidad mayor o igual a $\frac{1}{2} + \frac{1}{6}$. Además se entrega una demostración formal de que la probabilidad de que el adversario gane el juego es mayor o igual a $\frac{1}{2} + \frac{1}{6}$.