Pontificia Universidad Católica de Chile
Departamento de Ciencia de la Computación
IIC3253 - Criptografía y Seguridad Computacional

Tarea 1

28 de Abril de 2022

1º semestre 2022 - Profesores: M. Arenas, M. Ugarte
Nombre: Jorge Schenke Larraín. n° alumno: 17641624.

P2

- Supuesto: Para un bit cualquiera de la llave, el cambio de ese bit producirá un cambio en un bit específico del mensaje cifrado (Como OTP).

Cómo ganar:

1. El adversario encripta $m = 0^n$ con una llave prohibida como $k = 0(1)^{n-1}$.

   El objetivo de este ejercicio es definir qué bit del cifrado se ve afectado por el 0 inicial de la llave. Ya que todos los bits del mensaje son iguales, el cifrado tendrá todos sus bits iguales menos 1, el cual será el bit asociado al primer bit de la clave.

   Supongamos que todos los bits del cifrado c son 0 menos el que está en el índice i que es 1 (También podría hacerse el análisis en caso contrario, todos son 1 menos el i que sería 0). Con esto, podemos concluir que para toda llave válida, para $m = 0^n$ (como en nuestro ejemplo) el valor del bit i en c nunca será 1 si se hizo la encriptación, ya que las llaves con inicio 0 están prohibidas.

2. Ahora, enviamos $m = 0^n$ al verificador y analizamos su respuesta:
   - Caso 1: Si el bit i del c' contestado por el verificador es 0, concluyo que está cifrando.
   - Caso 2: Si el bit i del c' contestado por el verificador es 1, concluyo que está permutando ya que la única forma de llegar a ese resultado a través de una

encriptación es utilizando una llave prohibida.

Probabilidad de ganar:

$P_{ganar} = 1 - P_{perder}$

La única forma de perder es que el adversario esté permutando y que la permutación retorne un c' con el bit $i = 0$. En este caso concluiríamos que el verificador está cifrando cuando en realidad está permutando.

- $P_{permutar} = \frac{1}{2}$
- $P_{c'_i=0} = \frac{1}{2}$. Es fácil notar que la mitad de las permutaciones tienen el bit $i = 0$ y la otra mitad tienen el bit $i = 1$
- $\therefore \mathrm{P}_{perder} = P_{permutar} \cdot P_{c'_i=0} = \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$
- $\therefore \mathrm{P}_{ganar} = 1 - P_{perder} = 1 - \frac{1}{4} = \frac{3}{4}$

$\therefore La probabilidad de ganar es significativamente mayor a 1_{\frac{1}{2}}$, por lo que este esquema no es una PRP