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.

P4

- La resistencia a colisiones se refiere a la probabilidad de que, para dos mensajes $(m_1 \neq m_2) \in M$ un algoritmo de hashing retorne el mimso resultado. Si esta probabilidad es despreciable, entonces el algoritmo es resistente a colisiones.

  Es importante notar que para cualquier algoritmo de hashing donde $|m| \gg |h|$ esta probabilidad siempre va a ser > 0 ya que existen mucha mayor cantidad de mensajes que de hashes posibles. Por principio de palomar, a lo menos un par de mensajes distintos retornará el mismo hash.

  Utilizando el ejemplo $Hash - Col$ visto en clases, es fácil encontrar un ejemplo de colisión:
  $h(m) = (A \times m + B) mod C$
  Con $A = 1$, $B = 0$ y $C = 2$ podemos ver que:

  - $h(0) = (0 \times 1 + 0) mod 2 = 0$
  - $h(2) = (2 \times 1 + 0) mod 2 = 0$

  Por lo que encontramos una colisión, pero la probabilidad de que dos mensajes aleatorios produzcan una colisión es bastante baja y depende del tamaño de los conjuntos de mensajes y hashes posibles:

  Consideremos: $n = |m|$ y $l = |h|$
  Número de colisiones: $\#_{col}(m1, m2) = \frac{2^n}{2^l} = 2^{(n-l)}$

  Probabilidad de colisión específica: $\frac{1}{2^{(n-l)}}$
  Por lo tanto $Hash - Col$ es resistente a colisiones.

- Un algoritmo de hashing es resistente a preimagen cuando la probabilidad de que dada una salida específica, se pueda encontrar el mensaje original que lo generó, es despreciable. Teniendo en cuenta este concepto, es fácil demostrar que un algoritmo resistente a colisiones es resistente a preimagen:

  Si sabemos que un algoritmo de hashing es resistente a colisiones, sabemos entonces que existen una gran cantidad de colisiones posibles para los conjuntos de mensajes y de hashes posibles ya que $|m| \gg |h|$.

  Ya que existen gran cantidad de colisiones posibles, sabemos que para un mismo hash, existen muchos mensajes que potencialmente purden haberlo producido, específicamente:

  Cantidad de mensajes posibles para un hash: $2^{(n-l)}$ (ver punto anterior)

  por lo tanto, la probabilidad de adivinar cual de todos esos mensajes era el original es la misma que encontrar dos mensajes aleatorios que tengan el mismo hash:

  Probabilidad de adivinar mensaje original: $\frac{1}{2^{(n-l)}}$

  Lo cual es una función despreciable, por lo que podemos concluir que es resistente a colisiones.

  $\therefore$ Resistencia a colisiones $\Rightarrow$ Resistencia a preimagen