Formalizando la noción de resistencia a colisiones

Considere una función de hash (Gen, h)

Definimos el juego $Hash\text{-}Col(n)$:

1. El verificador genera $s = Gen(1^n)$, y se lo entrega al adversario
2. El adversario elige mensajes m_1 y m_2 con $m_1 \neq m_2$
3. El adversario gana el juego si $h^s(m_1) = h^s(m_2)$, y en caso contrario pierde

Formalizando la noción de resistencia a colisiones

Una función de hash (Gen, h) se dice resistente a colisiones si para todo adversario que funciona como un algoritmo aleatorizado de tiempo polinomial, existe una función despreciable $f(n)$ tal que:

$$\Pr(\text{Adversario gane } \mathit{Hash\text{-}Col}(n)) \leq f(n)$$

¿Cómo se formaliza la noción de ser resistente a preimagen usando las ideas anteriores?

Usted va a contestar esta pregunta en la tarea 1

Y además usted va a demostrar que ser resistente a colisiones implica ser resistente a preimagen

¿Dónde estamos?

- Estudiamos dos conceptos fundamentales en criptografía: cifrado simétrico y funciones de hash
  - Vimos algunas propiedades teóricas de estos conceptos
- Vamos a estudiar un tercer concepto fundamental: autentificación de mensajes
  - También vamos a ver algunas de sus propiedades teóricas
- Después de esto vamos a ver cómo se pueden implementar estos conceptos en la práctica