Funciones de hash criptográficas

Función de un espacio de posibles mensajes a un espacio de mensajes de largo fijo:

$$h : \mathcal{M} \to \mathcal{H}$$

$\mathcal{M}$ es el espacio de mensajes y $\mathcal{H}$ es el espacio de posibles valores de la función de hash

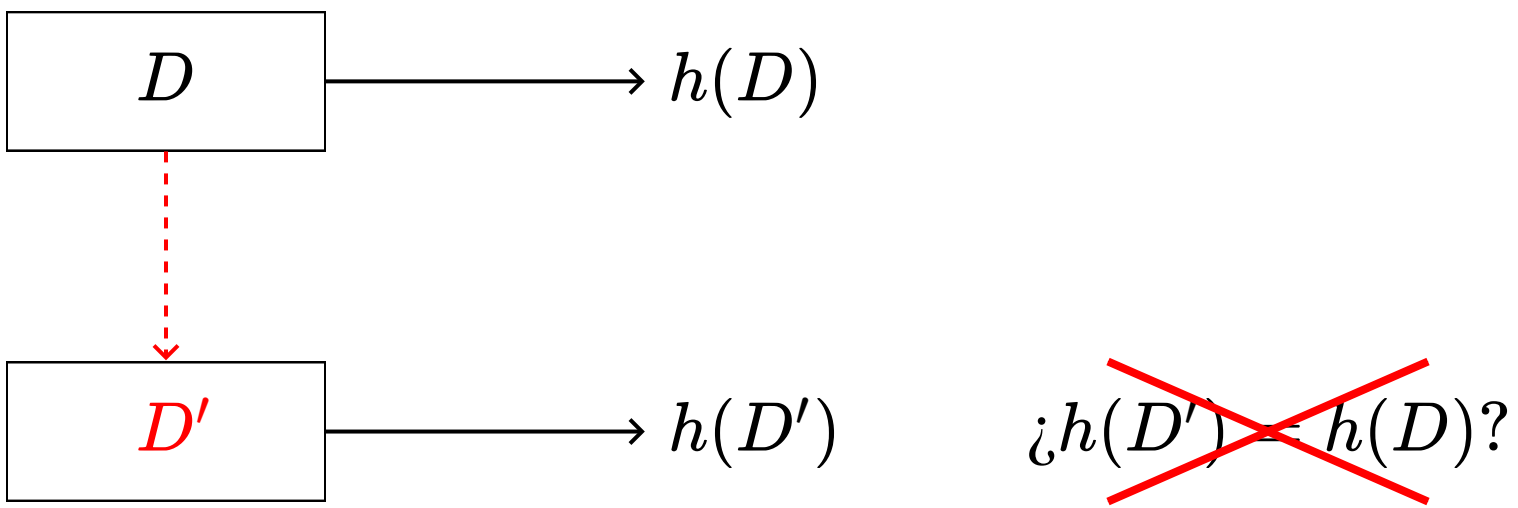
- Por ejemplo, $\mathcal{M} = \{0,1\}^*$ y $\mathcal{H} = \{0,1\}^{128}$
- Decimos que $h(m)$ es el hash de un mensaje m

Dos propiedades fundamentales de las funciones de hash

- Debe existir un algoritmo eficiente que, dado $m \in \mathcal{M}$, calcula $h(m)$
- No debe existir un algoritmo eficiente que, dado $x \in \mathcal{H}$, encuentra $m \in \mathcal{M}$ tal que $h(m) = x$

La segunda propiedad se denota como ser resistente a preimagen

Una primera aplicación: integridad de un documento



¿Por qué insistimos en el adjetivo "criptográficas"?

Considere la siguiente función de hash:

$$h(m) \ = \ (A \cdot m + B) \mod C$$

Suponemos que los mensajes son números naturales

- A, B y C son constantes, C es un número primo

¿Es esta función resistente a preimagen?