

Hashing resistente a colisiones

Una función hash sin clave resistente a colisiones es un mapa $H: M \rightarrow T$ de un mensaje largo M a un espacio digest T pequeño de tal forma que encontrar dos mensajes m_0 y m_1 con el mismo digest $H(m_0) = H(m_1)$ es difícil. Una función resistente a colisiones H es un lossy compressor que asigna una huella t a un mensaje m . Si tenemos $I = (S, V)$ que es un MAC seguro y H es resistente a colisiones, le MAC derivado: $I' = (S', V')$:

$S'(k, m) = S(k, H(m)) \rightarrow V'(k, H(m))$

es un MAC seguro.

From:
<http://knoppia.net/> - **Knoppia**

Permanent link:
<http://knoppia.net/doku.php?id=si:hrc>

Last update: **2024/10/15 15:16**

