Pregunta 4

Usando un juego como Hash-Col(n) definir la resistencia a preimagen

Demostrar que si (Gen, h) es resistente a colisiones, entonces es resistente a preimagen.

La resistencia a preimagen se define como la inexistencia de un algoritmo eficiente que, dado $x \in H$, encuentra un m tal que $h(m) = x$

Entonces defino el juego Hash-Pre(n):

1.- El verificador genera un $s = Gen(1^n)$ y un hash x creado a partir de un mensaje m. $h^s(m) = x$ y se los entrega al adversario

2.- El adversario elige un mensaje m'

3.- El adversario gana si $m' = m$

Demuestro por contraposición, si $p \rightarrow q$ entonces $\neg q \rightarrow \neg p$.

P.D: r. a colisiones $\longrightarrow$ r a preimagen

Asumo que (Gen, h) NO es resistente a preimagen, por lo que existe un algoritmo eficiente tal que dado un $x \in H$ encuentra un $m \in M$ tal que $h(m) = x$

Consideremos un $x \in H$ creado de la siguiente forma

$$h(m) = x$$

Como sabemos que $h^{-1}(x)$ no es una operación costosa es posible asumir que si existe un $m' \neq m$ tal que $h(m') = x$ este tampoco es costoso de encontrar

Por lo tanto el (Gen, h) no es resistente a colisiones.