11/10/22 **Strong Collision Resistance:-**

Given H, S, A can't find an x & x', s.t.; $x \neq x'$ and $H^S(x) = H^S(x')$.

11/15/22: **Merkle - Damgård Transform:-** For constructing hash Function from data compression Function

$$\underbrace{D}_{n\text{-bits}} \leftarrow H(S, x)$$

Let $n = 8$; $2n$; $|x| = 14$, $|x_1| = 7$, $|x_2| = 7$ bits

$$B = \lceil 14/8 \rceil = 2 \text{ blocks}$$

set $x_{B+1} = x_3 = |x| = 14$.

set $z_0 = 0^n$.

For, $i = 1$: $z_1 = h(z_0 \| x_1)$

$z_2 = h(z_1 \| x_2)$

$z_3 = h(z_2 \| x_3)$

The size of $|z_1| = |z_2| = |z_3| = n$-bits.

And Hence, $D = z_3$

Return D.

Small-Space Birthday Attack :- (Slide No: 21)

$i=3$,

$x_3 = x_6 \mid x_i = x_{2i}$
$i=3$

Find J, such that,

$x_J = x_{3+J}$

$\therefore J = 3.$

Extra Credit: why is the space complexity

Constant time $O(1)$? Explain?

Inverted Hashes :-

11/17/22: Smart Way 1 :-

Lookup Table to find x.

Key	Value
x	$H(x)_1$
$H(x)_1$	$H(x)_2$
$H(x)_2$	$H(x)_3$
$\vdots$	$\vdots$
$H(x_{2^\lambda - 1})$	$H(x_{2^\lambda})$

y, y', y''

2^L digests

$H(y) = z$

If $z \stackrel{?}{=} H(x_i)$,
return $H(x_{i-1})$ | $H(x_{i-1}) = y$.

with Pre-processing:-

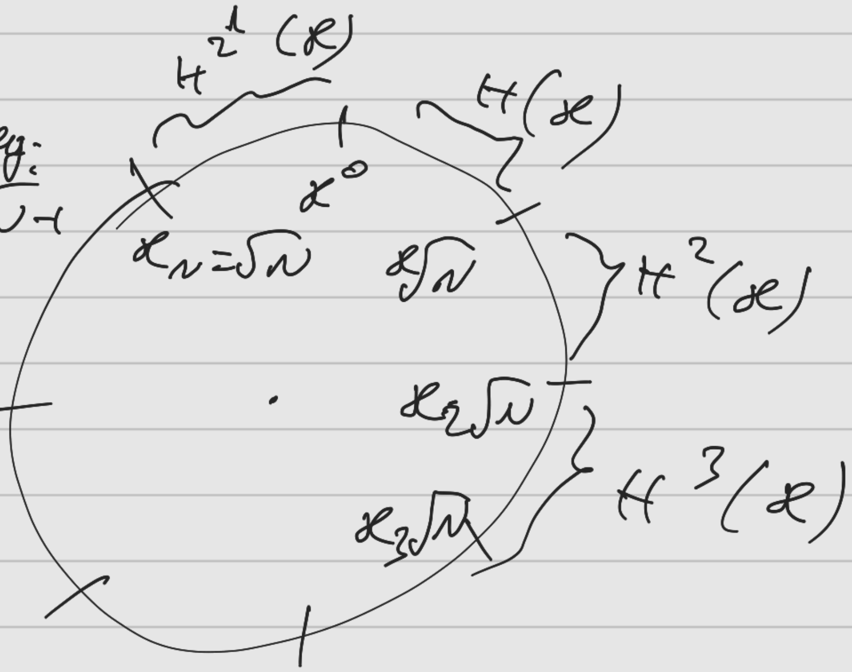
Time: $O(2^L) + \underbrace{O(1)}_{H(y)=z} + \underbrace{O(1)}_{\text{lookup } z}$

without preprocessing:-

Time: $O(1) + O(1) = O(1)$

Smart way 2:

Last seq:
$x = \sqrt{N}-1$



$x(\sqrt{N}-1)\sqrt{N}$
$= x_{N-\sqrt{N}}$

$x(\sqrt{N}-1+1)\sqrt{N}$
$= x_N$

Seg	St, end points
$H(x)$	$(x_0, x\sqrt{N})$
$\vdots$	$\vdots$
$H_2^{l}(x)$	$(x_N - \sqrt{N}), x_N$

size $\sqrt{N}$

Baby steps:-

End point : e.g, $x_3\sqrt{N}$

Start point: $x_2\sqrt{N}$

$H(x_2\sqrt{N}) = z$

$H(z) = z'$

$H(z') = \ldots\ldots$

$\vdots$

$H(x_3\sqrt{N}) = z_N$

check If $\{z, z', \ldots\} = y$.

The Time Complexity is,

$$O\sqrt{N} + O\sqrt{N} = O(2\sqrt{N}) \Rightarrow O(\sqrt{N})$$

and the space complexity is,

$$O(\sqrt{N}).$$

Random Oracle (RO) model :-

$$H : \{0, 1\}^* \longrightarrow \{0, 1\}^\infty$$