# Merkle - Damgrad Hashing

Defⁿ :- It is a method of building collision resistant hash fxns using one-way compression fxns.

proof of security :- There are 2 cases based on L:

Case-1 ($L \neq L_x'$)

For last steps: $H^S(x) \rightarrow Z_{B_{11}} = h^S(Z_B \| L)$

$H^S(x') \rightarrow Z'_{B'+1} = h^S(Z'_{B'} \| L')$

$\because h^S(Z_B \| L) = h^S(Z'_{B'} \| L')$ $[H^S(x) = H^S(x')]$

but $L \neq L'$ $\therefore$ $Z_B \| L$ & $Z'_{B'} \| L'$ are different, hence there is a collision of 2 different strings.

Case-2 ($L = L'$)

$\therefore$ $B = B'$, $x_{B+1} = x'_{B+1}$

$\because$ $x \neq x'$ & $|x| = |x'|$,

there exists at least one $i$ such that $x_i \neq x_i'$

Let $i \leq B+1$ be the highest index s.t.

$Z_{i-1} \| x_i \neq Z'_{i-1} \| x_i'$

If $i^* = B+1$, then $Z_B \| x_{B+1}$ and $Z'_B \| x'_{B+1}$ are different.

$\because h^S(Z_B \| x_{B+1}) = Z_{B+1} = H^S(x) = H^S(x')$

$= Z'_{B+1} = h^S(Z'_B \| x'_{B+1})$

If $i^* \leq B$, then maximality of $i^*$ implies $Z_{i^*} = Z'_{i^*}$

$\therefore$ $Z_{i-1} \| x_i$, & $Z'_{i-1} \| x_i'$ are different & just a collision.