used in MD5, SHA-1/2, ...

Merkle-Damgard:

compression function $\rightsquigarrow$ hash

$\tilde{H}: \underbrace{b+c}_{\text{bits}} \to \underbrace{b}_{\text{bits}}$ $\qquad$ $H: \underbrace{\text{any}}_{\text{bits}} \to \underbrace{b}_{\text{bits}}$

THM: $\tilde{H}$ collision-free $\Rightarrow$ H collision-free

$H(x)$: $x = \underbrace{x_1}_{c}\underbrace{x_2}_{c} \cdots \underbrace{x_n}_{c}$

$h_1 = 0$ — or any other ...

$\underbrace{h_{i+1}}_{b} = \tilde{H}(\underbrace{h_i}_{b}, \underbrace{x_i}_{c})$

$\Rightarrow h_{n+1} =: H(x)$

EG

x	000	001	010	011	100	101	110	111
$\tilde{H}(x)$	00	10	11	01	10	00	01	11

compresses $\underbrace{3}_{2+1=b+c} \to \underbrace{2}_{b}$

$H(1101) = ?$ $\qquad$ using MD with $h_1 = 0$

$x = x_1 x_2 x_3 x_4$ $\quad (1\ 1\ 0\ 1)$

$h_1 = 00$

$h_2 = \tilde{H}(h_1, x_1) = \tilde{H}(00, 1) = 10$

$h_3 = \tilde{H}(h_2, x_2) = \tilde{H}(10, 1) = 00$

$h_4 = \tilde{H}(h_3, x_3) = \tilde{H}(00, 0) = 00$

$h_5 = \tilde{H}(h_4, x_4) = \tilde{H}(00, 1) = 10 = H(1101)$

example collision: $H(1) = H(1101)$