SHA - 2

256 biți

pachete de 64 biți -> livrat pe 512 biți

mesaj de l biți -> extinderea ->

-> un bit de 1

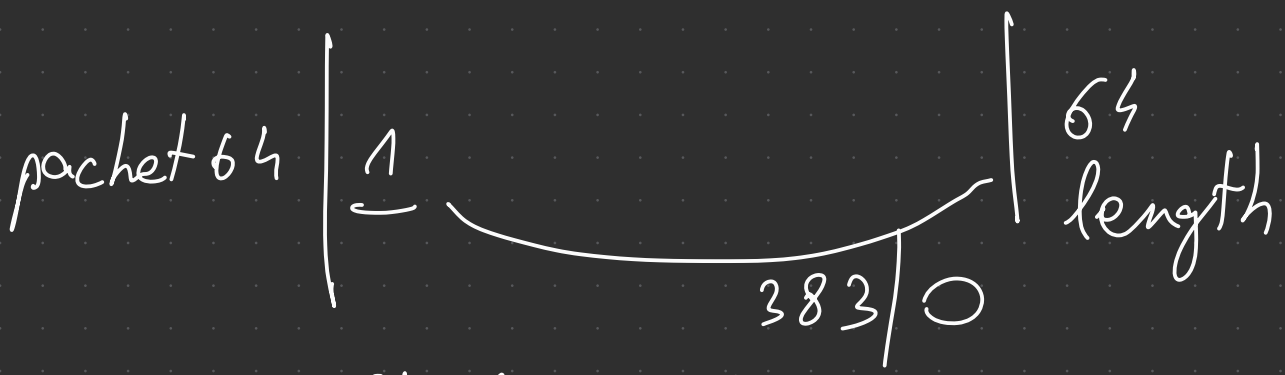
k biți de 0 a.î. $l+1+k = 448$

valoarea lui l pe 64

abcd0123 -> pachet

$8 \cdot 8 = 64$ -> $l = 64$ (40_{hex})

ASCII



$512 - 64 - 64 - 1 = 383$

72 char -> 64 + 8

reg fl → 8 × 64 → 512 blk
regs len