

SHA-2

256 biti

pachete de 64 biti \rightarrow livrat pe 512 biti

mesaj de l biti \rightarrow extinderea \rightarrow

\rightarrow un bit de 1

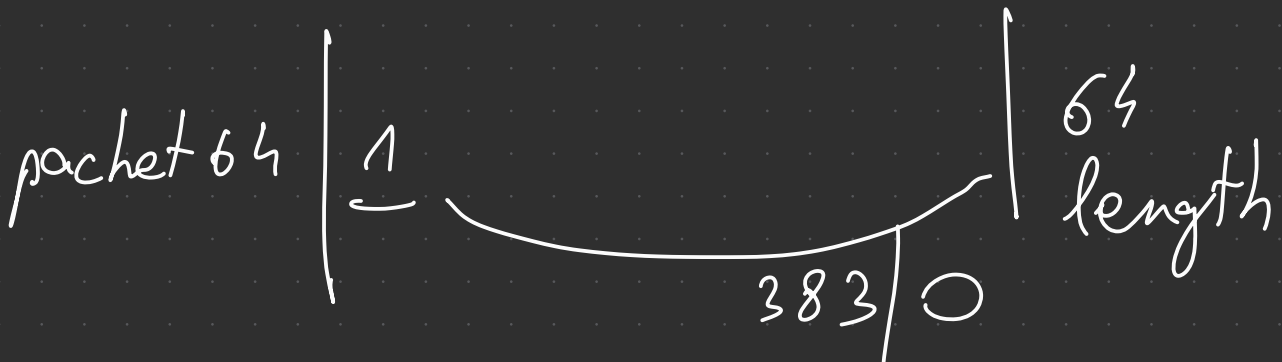
k biti de 0 cu $l+1+k=448$

valoarea lui l pe 64

a b c d 0123 \rightarrow pachet

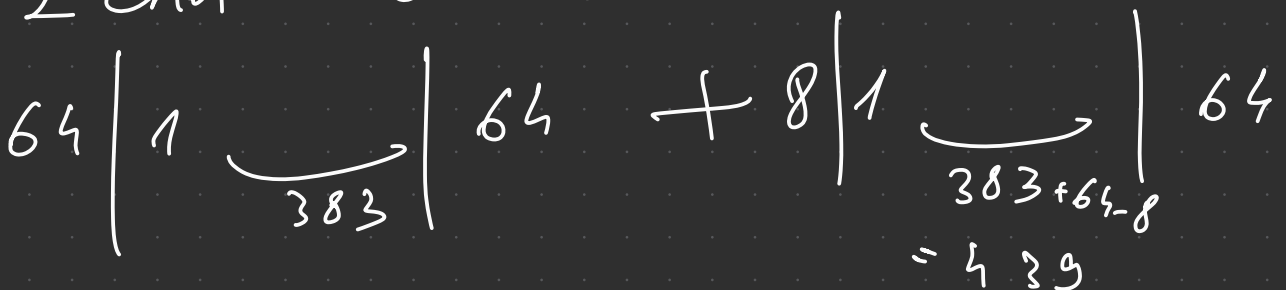
$8 \cdot 8 = 64 \rightarrow l = 64$ (40 hex)

ASCII



$$512 - 64 - 64 - 1 = 383$$

72 char $\rightarrow 64 + 8$



reg fl \rightarrow 8 x 64 \rightarrow 512 blk
regs len