

for string:

0xFFE00000 0x1FFC00 0x3FF

ex:  $y = b'1100\ 0101\ 0110\ 0110\ 1010\ 1111\ 0111\ 0010$

0x C 5 6 6 A F 7 2

Step 1:  $y \wedge (y \gg 4) = y \wedge (y \gg 11) = (s1)$

$\Rightarrow$

1100 0101 0110 0110 1010 1111 0111 0010

0000 0000 0000 1000 1010 1100 1101 0101

(s1) = 1100 0101 0111 1110 0000 0011 1010 0110

0x C 5 7 E 0 3 A 6

$\Rightarrow$  To undo:  $y =$

Step 2:  $y \wedge [(y \ll 5) \wedge B] = (s1) \wedge [(s1) \ll 5] \wedge B = (s1) \wedge [(s1) \ll 7] \wedge 0x9D2C5680 = (s2)$

$\Rightarrow ((s1) \ll 7) \wedge 0x9D2C5680 = (s2)$

$\Rightarrow$

1011 1111 0000 0001 1101 0011 0000 0000

1001 1101 0010 1100 0101 0110 1000 0000

(s1)  $\Rightarrow$  1100 0101 0111 1110 0000 0011 1010 0110

(s2) = 0101 1000 0111 1110 0101 0001 1010 0110

5 8 7 E

Step 3:  $y \wedge [(y \ll 7) \wedge C] = (s2) \wedge [(s2) \ll 15] \wedge 0xFFC60000 = (s3)$

0010 1000 1101 0011 0000 0000 0000 0000

$\wedge$  1110 1111 1100 0110 0000 0000 0000 0000

(s2) = 0010 1000 1100 0010 0000 0000 0000 0000

(s3) = 0111 0000 1011 1100 0101 0001 1010 0110

0x 7 0 E C 5 1 A 6

Step 4:  $y \wedge (y \gg 4) = (s3) \wedge ((s3) \gg 18)$

0000 0000 0000 0000 0001 1100 0010 1111

$\wedge$  0111 0000 1011 1100 0101 0001 1010 0110  $\rightarrow (s3)$

(s4) 0111 0000 1011 1100 0100 1101 1000 1001

0x 7 0 B C 4 D 8 9

Inverting

(s4)  $\rightarrow$  (s3):  $(s3) = (s4) \wedge (s4 \gg 4)$

(s3)  $\rightarrow$  (s2):

01 1000 0111 1110 0101 0001 1010 0110

(s3)  $\wedge [(s3) \ll 7] \wedge C$  (s3)  $\wedge [16:7] \wedge 0x0000$

(s2)  $\rightarrow$  (s1):

1100 0101 0111 1110 0000 0011 1010 0110

(s2)  $\wedge [(s2) \ll 5] \wedge B$  (s2)  $\wedge [(s2) \ll 5] \wedge 0$  (s2)  $\wedge 0$

s1d s1c s1b s1a

(s1)  $\rightarrow y$ :

1100 0101 0111 1110 0000 0011 1010 0110

$y^1 = s1$   $y^2 = (s1) \wedge (y^1 \gg 4)$   $y^3 = (s1) \wedge (y^2 \gg 4)$