

Quiz 2 - Will post sols Tues.
Should hand back Wed.

Today: Coding bitwise operators

⇒ Modern Crypto w/ Computers

Everything is 0/1s

Common ops on bitstrings

or $x \mid y$

$$\begin{array}{r} \begin{array}{cccccc} 5 & 4 & 3 & 2 & 1 & 2^0 \\ 2 & 2 & 2 & 2 & 2 & 2 \end{array} \\ 001011 = 11 \\ 010010 = 18 \\ \hline 011011 = 27 \end{array}$$

and $x \& y$

$$\begin{array}{r} 001011 = 11 \\ 010010 = 18 \\ \hline 000010 = 2 \end{array}$$

xor $x \wedge y$

$$\begin{array}{r} 001011 = 11 \\ 010010 = 18 \\ \hline 011001 = 25 \end{array}$$

What is $x \wedge x = 0$

if we "encrypt" some plaintext, p ,
with key x

$$c = [p \wedge x]$$

$$p = c \wedge x$$

ONE TIME
PAD

$$\begin{aligned} (p \wedge x) \wedge x &= p \\ &= p \wedge (x \wedge x) \\ &= p \wedge 0 \end{aligned}$$

① cyclic bitshift

$10101110 \Rightarrow 01011101$

② permutation

unsigned int x;
3 31 0 5 ...

array
32 bit

bit shift

$x \gg 1$ (right shift)

$1011 \gg 1 \Rightarrow 101$

chops off least significant bit
(int div by 2)

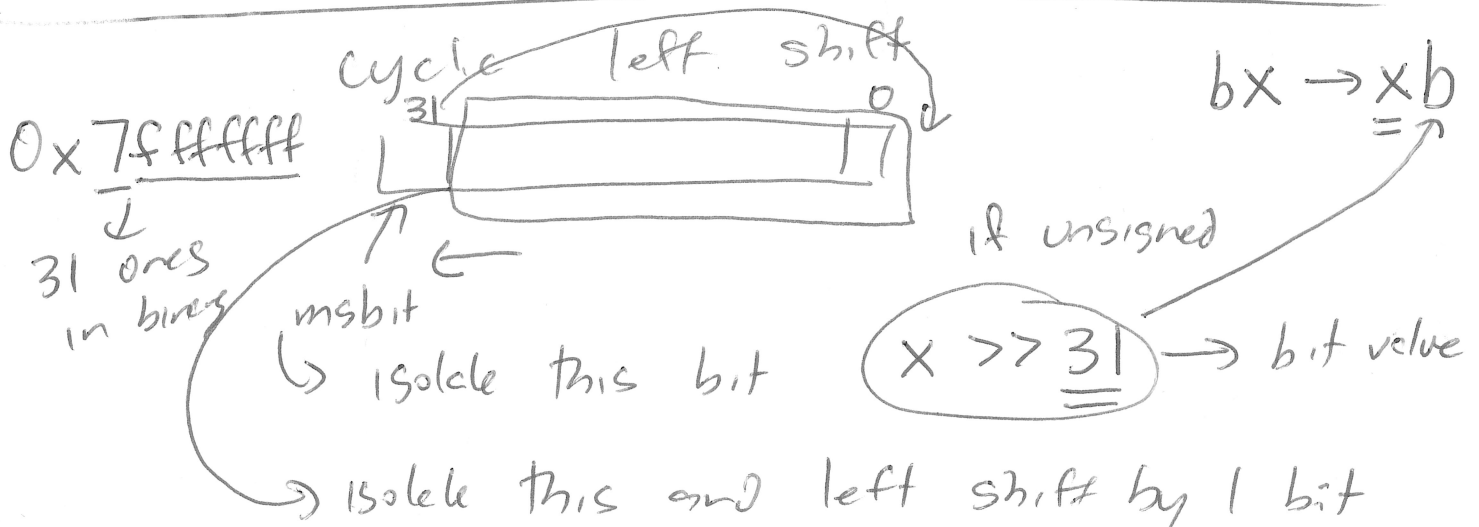
$x \gg k$ right shift of k bits

$x \ll 1$ (left shift)

mult by
2

$10111 \ll 1 \rightarrow 101110$

$x \ll k$ (left shift by k bits)
 $\hookrightarrow \text{mult } 2^k$



80002402

1000 0000 0000 0000 0010 0100 0000 0010 0

0000 0000 0000 0000 0100 1000 0000 0101

0 0 0 0 4 8 0 5

permutation on some bits

~~0 1 2 3 3~~

Input :

~~0 1 1 0 1 0 1 1~~

~~0 1 2 3 4 5 6 7~~

~~7 6 5 4 3 2 1 0~~

Store backwards

perm

~~6 2 0 1 7 5 3 4~~

~~1 0 1 1 0 1 0~~

~~1~~

tells you which bit to grab

Permutation Example

Input

1	0	1	0	0	1	1	1
---	---	---	---	---	---	---	---

0 1 2 3 4 5 6 7

perm

6	2	0	1	7	5	3	4
---	---	---	---	---	---	---	---

1 1 1 0 1 1 0 0

build backwards // $i = \text{index perm}, j = \text{bit value}$

for (int $i = 31$; $j = 0$; $i \geq 0$; $i--, j++$) {
 $31 - \text{perm}[i]$ // bitwise location

~~$31 - \text{perm}$~~
 $\text{tmp} = \text{Input} \& (1 \ll (31 - \text{perm}[i]))$
 $\text{tmp} \gg (31 - \text{perm}[i] - j)$

POSITION I want
this bit.