CIS3362 9/27/21

(1) Quiz - 12/12 for all on Hill
Will post sols later today
Returned Wed.

---

(2) Plan for Class When Gone

Fri -
Mon -] Will let you know on Wed.
Wed - Mike McAlpin

---

(3) Bitwise Ops

(4) DES intro

```
int x = 23;
int y = 14;
```

16+4+2+1 ⇒ 0000...010111
8+4+2 ⇒ 000...001110
11001 = 25
(also addition mod 2 for each column)

XOR (x ^ y)

1 flips a bit, 0 keeps it the same.

AND x & y

```
  10111
  01110
-------
  00110  = 6
```

OR x | y

```
  010111
  001110
--------
  011111  = 31
```

X = 23 10111

X >> 1

right shift of 1 bit

10111 >> 1 = 1011

(int div by 2)

(clips off the last bit)

X >> k

right shift of k bits

10111 >> 3 = 10

(int div by 2^k)

clips off last k bits

X << 1

left shift of 1 bit

10111 << 1 = 101110

(mult 2)

10111 << 3 = 10111000

left shift of 3 bits

mult by 2^3, more gen 2^k if we shift by k bits

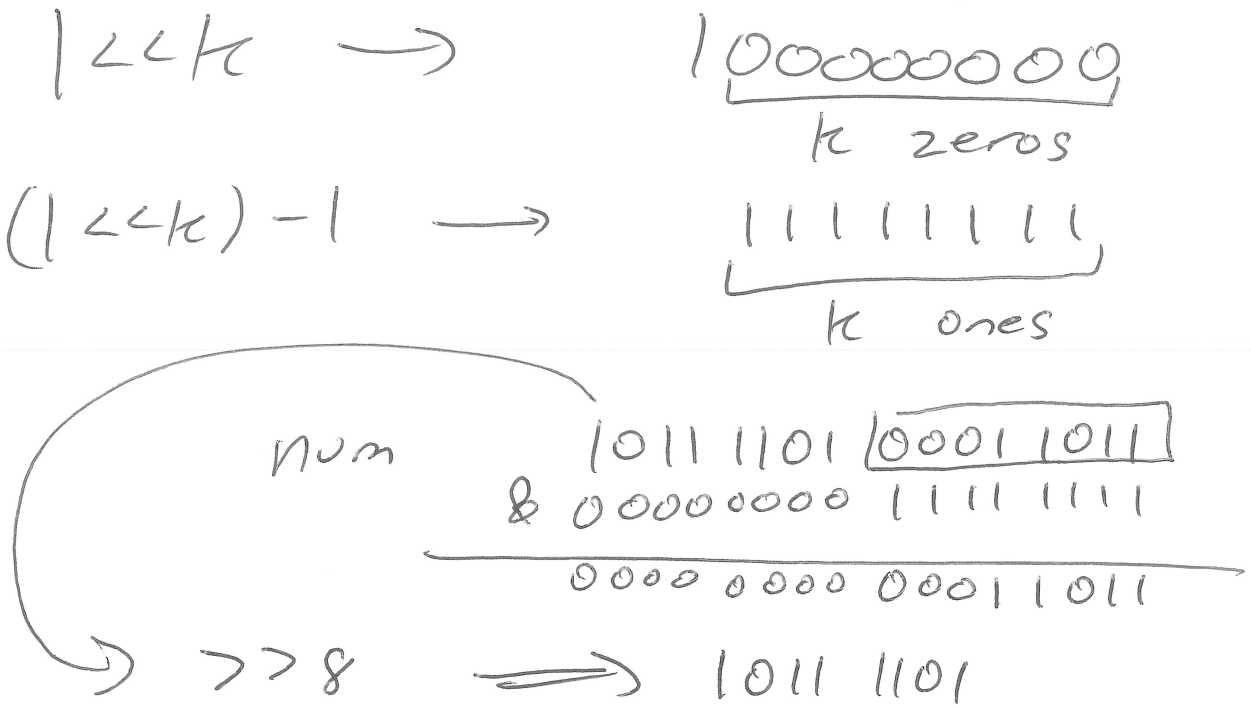
87_{16} = 10000111

$D8_{16}$ = 11011000

01011111

5F

0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
a	10	1010
b	11	1011
c	12	1100
d	13	1101
e	14	1110
f	15	1111


1<<k
1 0000000 0
k zeros
(1<<k)-1
1111111 11
k ones
num
1011 1101 0001 1011
& 0000 0000 1111 1111
0000 0000 0001 1011
>>8
1011 1101

DES (Modern Symmetric Key Ciphers)

US govt looking for encryption standard

Contest

Winner - IBM (Horst Feistel) written algorithm in house.

Structure: 64 bit blocks of plaintext

- 56 bit key
  - to create 16 Round keys of 48 bits

$$X \to IP(x) \to C_1 \to C_2 \to \cdots \to C_{16} \to IP^{-1}(C_{16})$$

- X: Plain
- $IP(x)$: reorders bits
- C_1: mix shift up using RK_1
- C_2: mix shift up using RK_2
- C_{16}: Ciphertext

Round happens 16 times - mostly simple operations.

ONLY non-linear part: S-BOXES.

- NSA made modifications to S-BOXES.
  - But largely, many believe that these modifications we made to make DES stronger against differential cryptanalysis.

Govt Standard from 1977 - 1999

Data Encryption Standard

~ 1997 DES challenge → took 3 months to get key.