CIS 3362 9/22/2025

Bitwise Operators

Usually store plaintext as a bitstring

P = "0110 1101" (1 byte)

blocks of bits (always multiple of 8)

DES uses ~~56~~ 64 bit blocks (key is 56 bits)

AES uses 128/192/256 bit blocks

logical operations are common to do bit by bit

```
x    0110 1101
y    1100 0111
and & 0100 0101
or  | 1110 1111
xor ^ 1010 1010
```

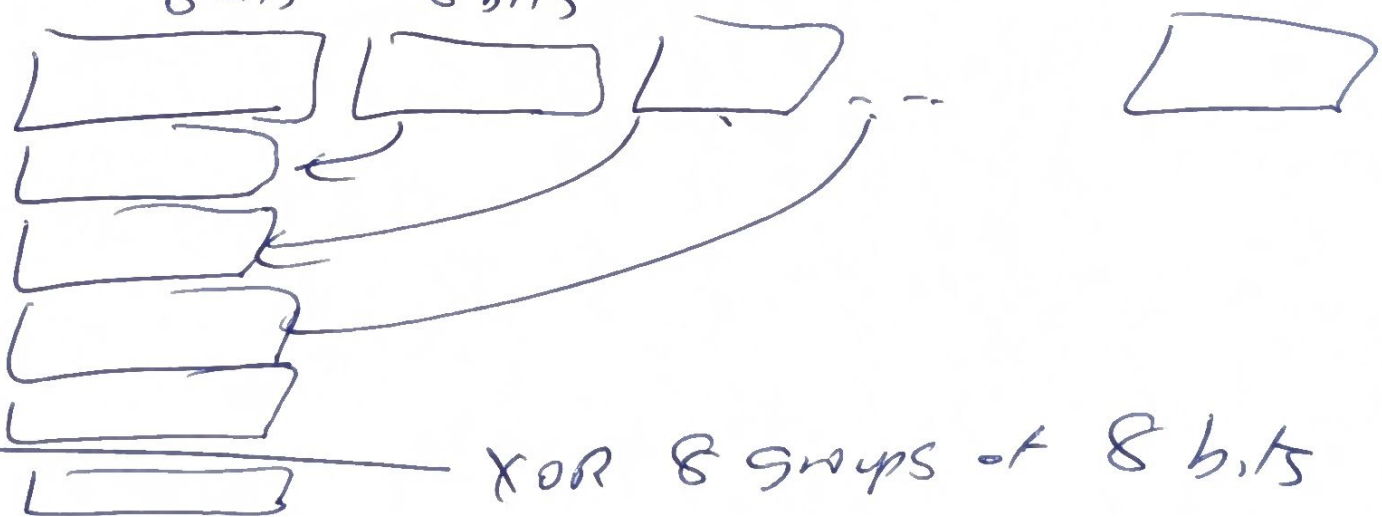
logical operations by bits

X << 4 → 0110 1101 0000

Left Shift (move # over 4 bits to left w/0 on right end)

X >> 4 → 0110 (chop off 1101)

64 bits — 8 bits — 8 bits



```
 10101101
&00100000
---------
 00T00000
```

XOR 8 groups of 8 bits

(1 << n) - 1 will have n least sign bits ON

$$\begin{array}{r} 1000 \\ -\ \ 1 \\ \hline 111 \end{array}$$