CIS 3362 9/26/22

1) Quizzes back on Wednesday!
1.5) Will release more info about Hmk 3B today. (announce)
2) Next Part of Course: Modern Cryptography (With COMPUTERS)

a) Symmetic / Private Key — Next portion

b) Public Key — Portion after that

Private Key - you + msg recipient share a private key that no one else has.

Most private key (modern) schemes are block ciphers - Plaintext is separated into chunks of n bits (0/1s), so n is what we call the block size.

Plaintext: 10110000 01001101 00111111 11011001

To manipulate bits in the computer, it's really helpful to know about bitwise operators.

Most important for crypto XOR ^ operator in code

bitwise XOR

```
a = 1001 0011
^ b = 0101 1001
-------------
    1100 1010
```

128+16+3 = 147

64+16+9 = 89

(exclusive or means exactly 1 of the 2 items is true)

XOR "flips" the bits where there is a 1.

```
  a = 1001 0011
^ a = 1001 0011
-------------
    0000 0000
```

a ^ a = 0

inverse operation of "XOR by a" is "XOR by a"

```
  a = 1001 0011
& b = 0101 1001
-------------
    0001 0001
```

↑ bitwise and

```
  a = 1001 0011
| b = 0101 1001
-------------
    1101 1011
```

↑ bitwise or

common use

a >> 4

↓ right bit shift

1001 | 0011 ⇒ 1001

↓ chop off

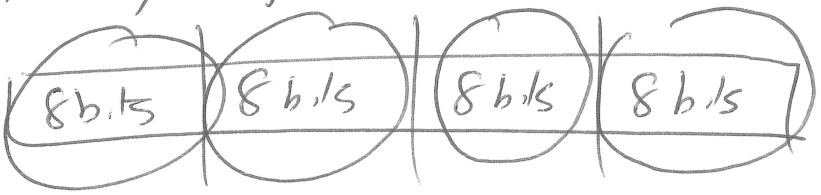
a << 4

↓ left bit shift

10010011 0000

Sample Code

1) taking several ints, breaking them up byte by byte and XORing each byte



a) extract 8 least significant bits

$$(1 << 8) - 1$$

$$100000000 - 1 \rightarrow 11111111$$

b) bitwise AND with this