CIS 562

for your grade

H1, H2, Q1, Q2
1% 3% 10% 10%
pts

$[(H1+H2)/25 + (Q1+Q2)/15]/.24$

A	85%	21
B	69%	38 → 70%
C	45%	67 → 50%

Primary Reason distribution is attendance.

Bitwise Operators in Computer

Private Key (Modern) Encryption (on computer)

Computer Data Abstract Form

bit strings split up into blocks

DES - 64 bit blocks [subdivide into 4-bits, 6-bits, 32-bits 48-bits, etc.]

AES - 128 bit, 192 bit, 256 bit
byte level (8 bits)

int 47 = 0... 0101111

common operation XOR math ⊕
prog lang ^

plain = 01101010
key = 10101101

11000111

If you never use a key again (one time) and you use it in this fashion (key length = msg length) this is called a ONE TIME PAD and it's unbreakable.

bitwise and &

```
  01101010
* 10101000
----------
  00101000
```

bitwise or |

```
  01101010
| 10101000
----------
  11101010
```

block << 4

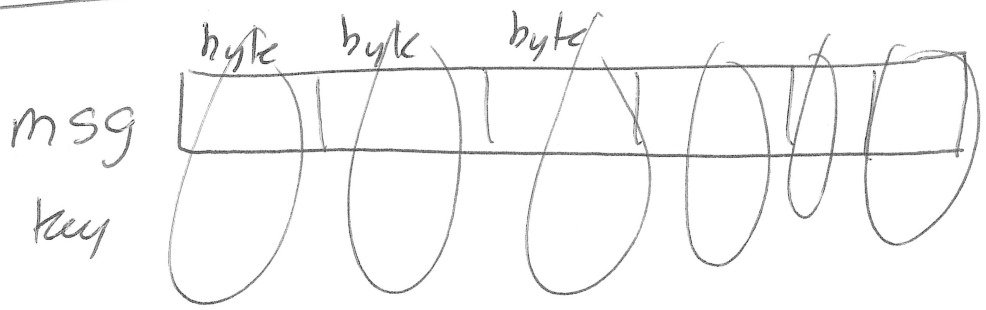
1011 << 4 ⟶ 10110000

↑

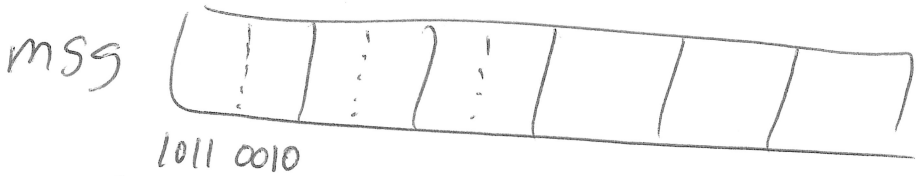
binary

block

11011001 >>4 → 1101



func XORs each array index w/ key and returns the result



1011 0010
⊕ 0010
1001

retrn XOR of each block of 4

---

35 00100011

77 01001101

01101110

block: 10110110
& 00001111
0000 0110

96+14 = 110

10110110 >>4
↳ 1011