

✓ ① Go over exam (probably A ~ 85%, B ~ 70%, C ~ 50%)

Next Part: Modern Symmetric Cryptosystems

- DES (64 bit plaintext blocks)
- AES (128/192/256 bit plaintext blocks)

"Symmetric" - "Private key cryptography"

2 people communicating SHARE a private key
that no one else knows → same model we're
thus far in the class.

Switch methods → COMPUTER
data is represented in binary!

~~And~~ Most of the algorithms simply assume
that the plaintext is a bit string.

Subdivide bit string into fixed block sizes,
and encrypt each block one by one.

A lot of the nuts + bolts of this class
of algorithms is bitwise operations.

8 - and

1 - or

^ - xor

>> - right shift

<< - left shift

180

42

&

1011 0100

0010 1010

1st

2nd

0010 0000

and

1 & 1 = 1

0 & 1 = 0

1 & 0 = 0

0 & 0 = 0

128

176

or

180

42 (1) or

190

10110100

00101010

10111110

1 1 1 = 1

1 1 0 = 1

0 1 1 = 1

0 1 0 = 0

1011 0100 180
1 0010 1010 42

1001 1110

158

128
144

254
64

One time pad

Plain text : 1011 1110

1 key : 0110 0010

1101 1100

Ciphertext

each plaintext is equally likely

$$(P \wedge K) \wedge K = P \wedge (K \wedge K) = P \wedge 0 = P$$

$$C_1 = (P_1 \wedge K)$$

$$\wedge C_2 = (P_2 \wedge K)$$

$$P_1 \wedge P_2$$

$$M \ll 3$$

$$M = 1011\ 0110$$

$$M \ll 3 = \boxed{1011\ 0110\ 000}$$

$$M \gg 2 = \boxed{101101} \mid \begin{array}{l} 10 \\ \text{chopped off} \end{array}$$

TASKS

① Counting the # of 1 bits

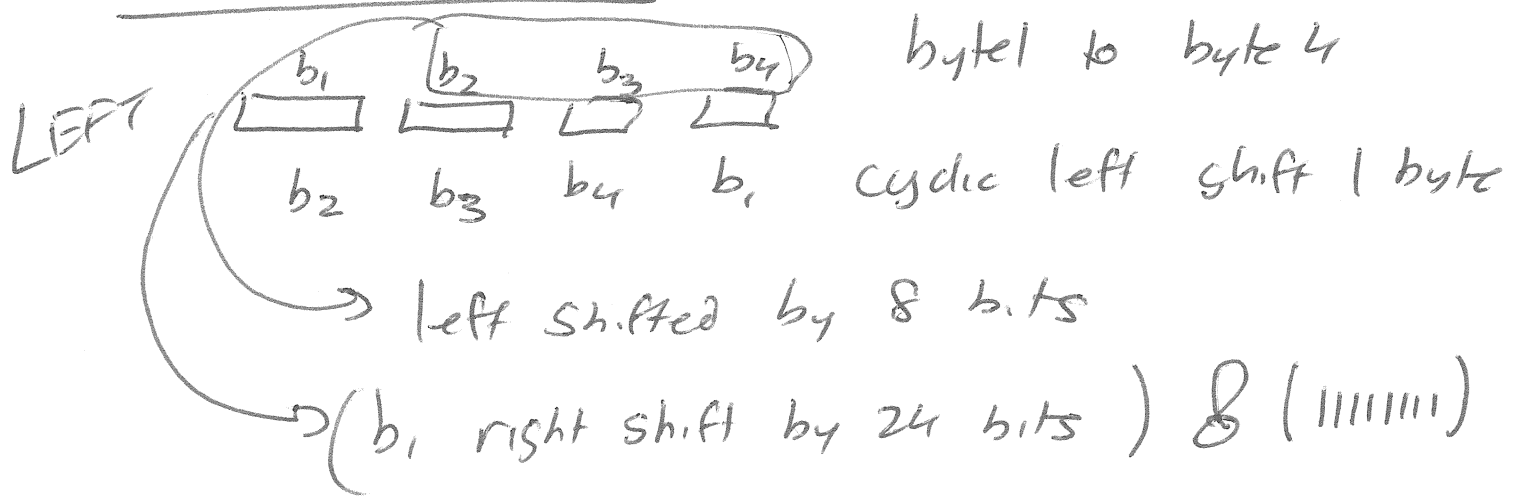
② Cyclic left shift, right shift

$$\begin{array}{r} \downarrow \\ \begin{array}{r} 1011\ \boxed{0}10 \\ \& \begin{array}{r} 0000\ 0\boxed{1}00 \\ \hline 00000\boxed{0}00 \\ 0 \end{array} \end{array} \quad \begin{array}{l} == 0 \\ ! > 0 \end{array} \quad \begin{array}{l} \text{bit off} \\ \text{bit on} \end{array}$$

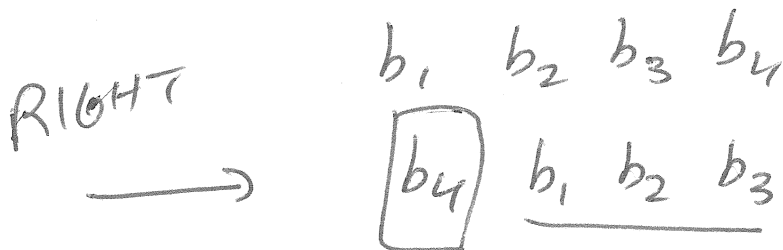
$$(1 \ll \hat{0}) \rightarrow$$

$$\begin{array}{c} 10000 \\ \underbrace{\hspace{1cm}} \\ \hat{0} \# \text{ of zeros} \end{array}$$

Cyclic Shift



$$\begin{array}{r}
 10000\ 0000 \\
 - \\
 \hline
 11111111
 \end{array}$$



$$\begin{array}{c}
 (b_4 \ll 24) + (num \gg 8) \oplus ((1 \ll 24) - 1) \\
 num
 \end{array}$$

XOR w/ key

Plaintext

int* msg,

int key



key =

msg[0] ^ key $\rightarrow$ CLS(key)

msg[i] ^ cyclekey

7 7 2 4 4 1 D C msg

0 7 5 b c D 1 5 key

7 0 7 F 8 C C 9

2 3 6 0 4 C 8 E

5 B C D 1 5 0 7

7 8 A D 5 9 8 9

1 0 1 1

1 1 0 0

1 0 0 1

1 1 0 0

1 0 1

1 0 0 1

1 0 1 1

1 1 0 0

1 1

1 1 0 0

1 0 1

1 1 1 0

1 1 1