

CITS 515. 9/25/2020.

Today: 1. go through hw1.  
2. Challenge.

---

Prob 1. Size of input =  $\log_2 n + \log_2 p + \log_2 f$ .

---

Remark.  $\log_2 n$  = the # of bits you need to rep.  $n$  in memory.

Be careful:

① Sometimes, Sugrueers don't care. Ex-ple:

Fib (int n) { // Fibonacci

!

return Fib(n-1) + Fib(n-2);

}

not size.

What's the running time? Let  $N = n$ .

Then the time is  $O(2^N)$ .

---

Actually, (!) let  $N = \log_2 n$ . The the

$\phi$  size.

time is  $O(2^{2^N})$ .

## ②. Problem RSA:

Given: number  $n$

Ques.:  $\exists p, q$  s.t.  $n = p \cdot q$  &  
 $p, q$  are primes?

---

Input size =  $\log_2 n$ . ✓

---

Engineers like to say: input size =  $n = N$ .  
Can you show: we have an  
alg to solve the RSA problem  
in poly-time on  $N$ ?

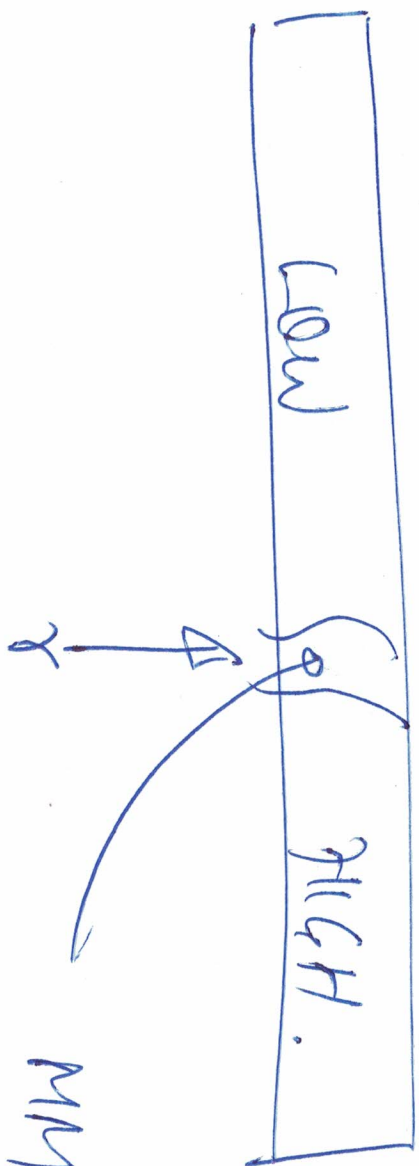
Yes.

Prob 2. Group Size = 3 and 7.



$\leftarrow$   $n/3$  groups  $\rightarrow$

$n/3$  medians.



we have  $\frac{1}{2} \cdot \frac{1}{3}n$  medians  $\leq MM$ .

each median is taken from a group of size 3.

so, we have 2 values  $\leq$  the median.

Therefore, in the original array, we have at  
least  $2 \cdot \frac{1}{2} \cdot \frac{1}{3}n$  values  $\leq MM$ .

$$\Rightarrow |Low| \geq \frac{n}{3} \quad \&$$

$$|High| \geq \frac{n}{3} \quad \&$$

$$|Low| + |High| = n$$

$$\Rightarrow |Low|, |High| \leq \frac{2}{3}n.$$

$$\Rightarrow \max \{ |Low|, |High| \} \leq \frac{2}{3}n.$$


---

$$T_w(n) = T_w\left(\frac{1}{3}n\right) + T_w\left(\frac{2}{3}n\right) + O(n)$$

Guess  $T_w(n) = O(n)$  for some  $c > 0$ .

Check:  $T_w(n) \leq c \cdot \frac{1}{3}n + c \cdot \frac{2}{3}n + a \cdot n$

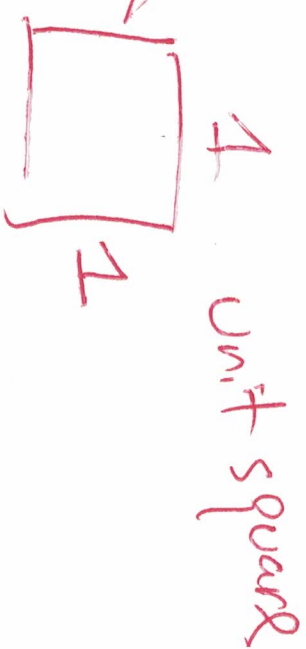
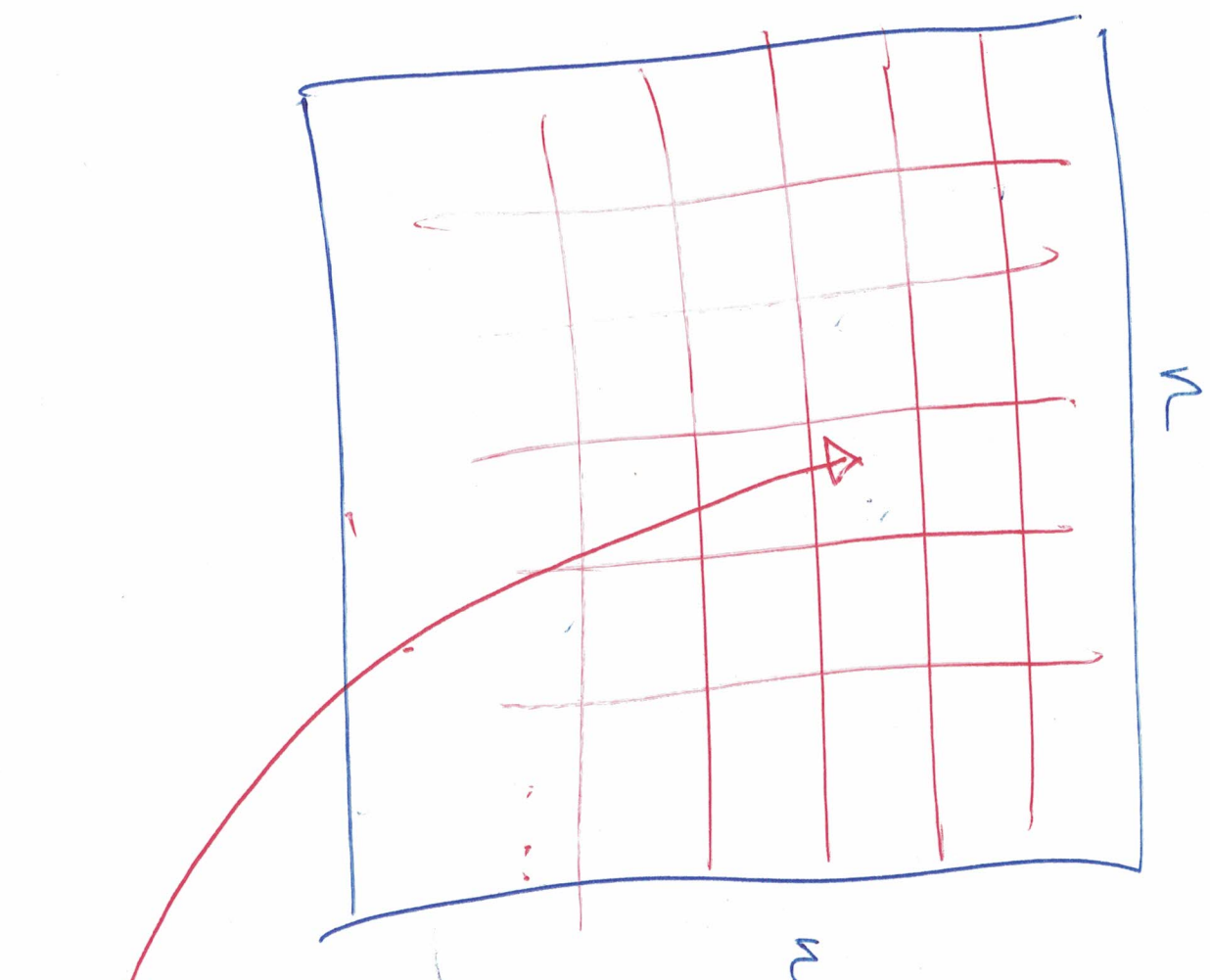
$$= c \cdot n + a \cdot n$$

$$\leq c \cdot n$$





Prob 3.



$N = n^2$  lines.  
any two  $\geq 1$   
lines true (in  $N$ )  
also for  
closest pair

I totally have  $n^2$  unit squares. Given the  $n^2$  bugs, we can see:

① each unit square contains exactly 1 bug,

or

② there is at least one unit square containing more than 1 bug.

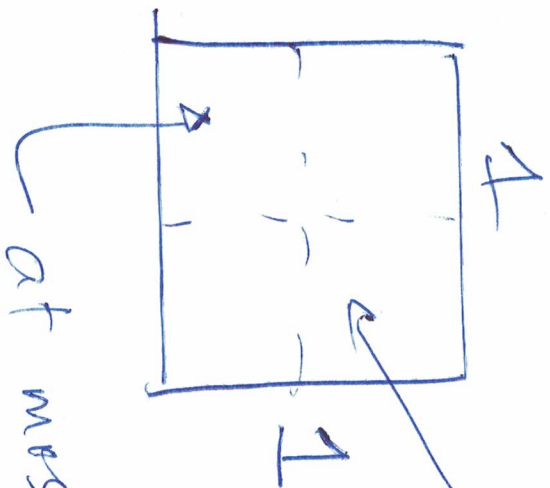
---

For case ①, closest pair can be found in linear time by searching, for each bug, all its neighboring squares.

→ the bugs in neighboring?



Case ②:



how many bugs you  
can max. fit in?  
at most 4.

at most 1 bug in this ~~sq~~  
half-square.

⇒ you can still search for the  
closest pair, by searching for each  
bug, all the bugs in its neighborhood  
if squares, bounded by a fixed number!

Prob 4.

white box program



graph



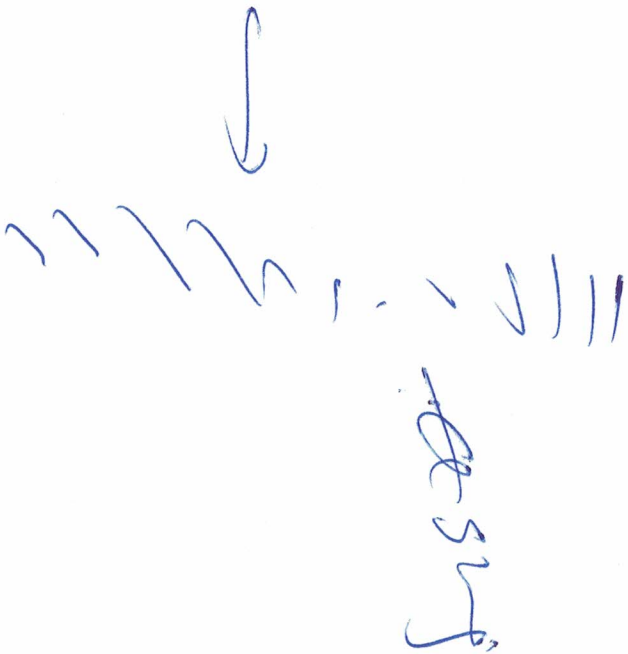
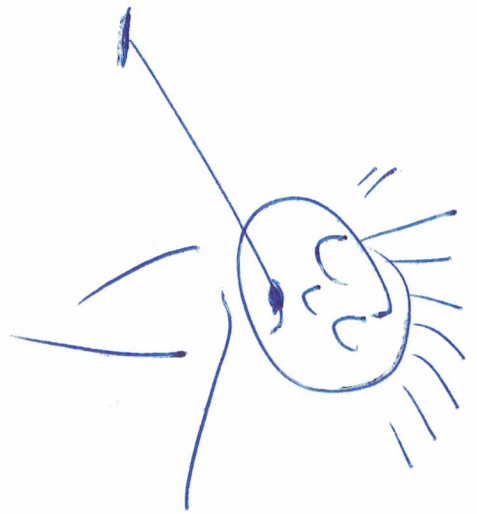
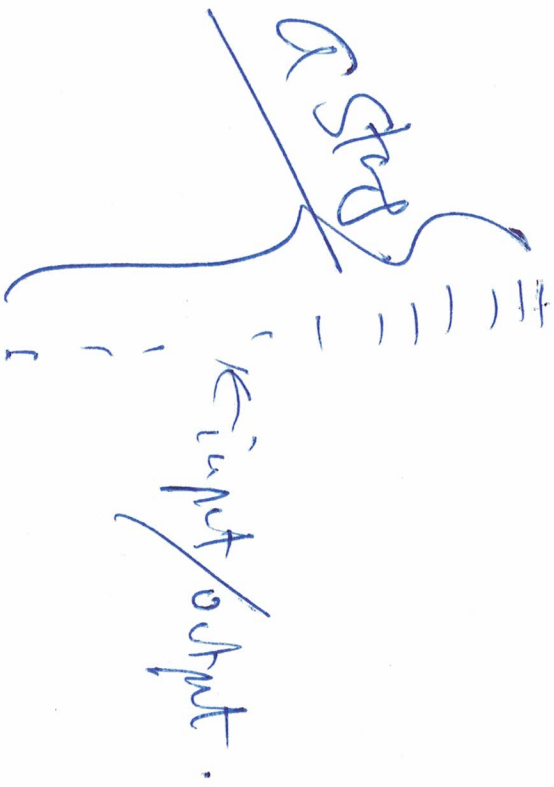
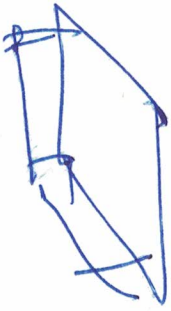
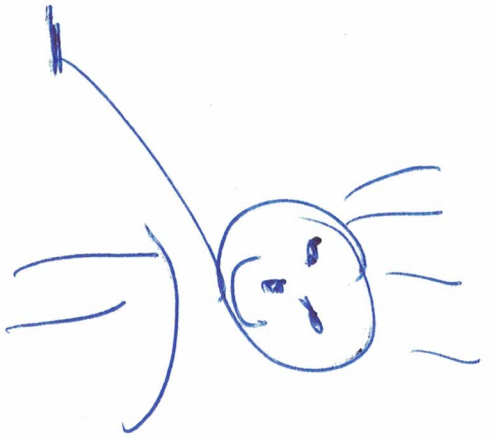
graph

soundly.

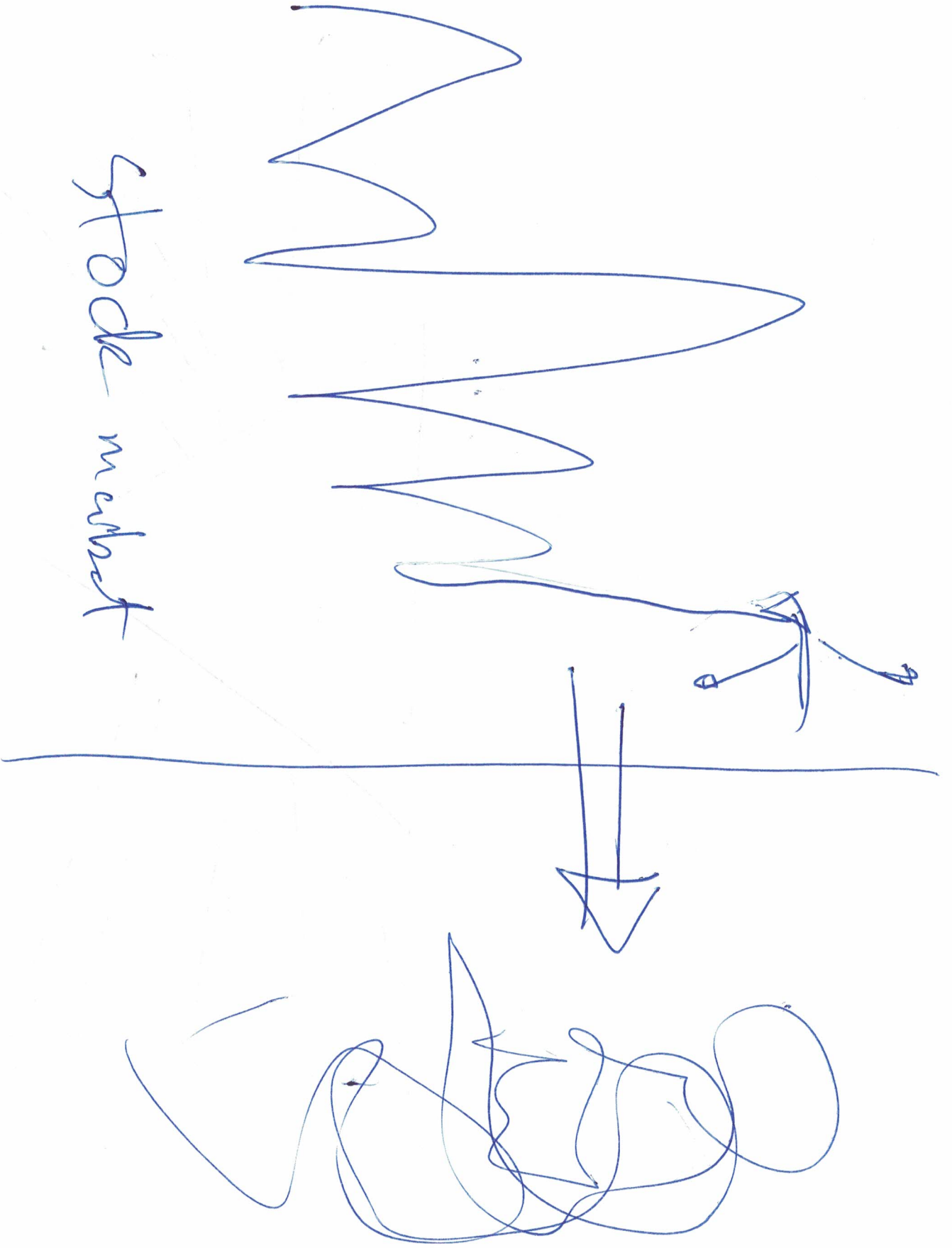


black box program





stock market



Given. two sets of strings.

A      B

---

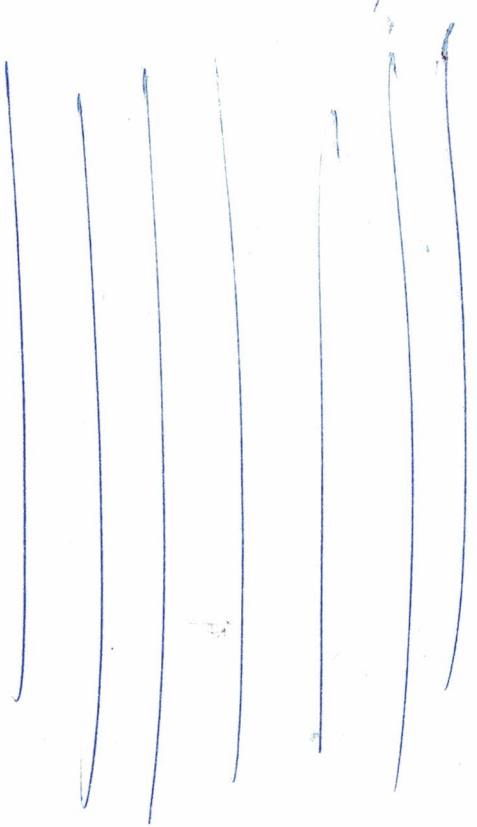
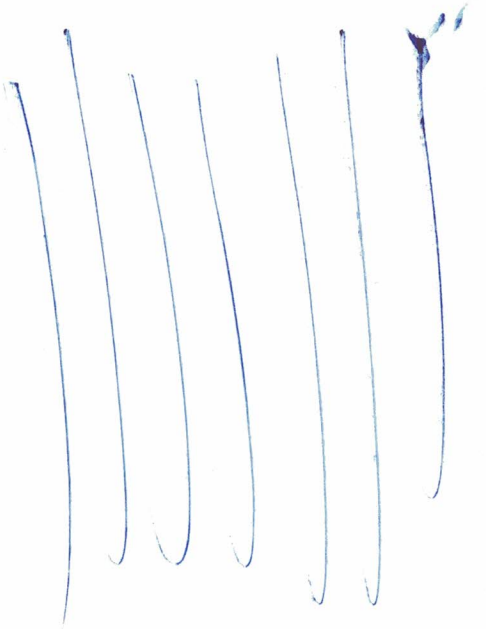
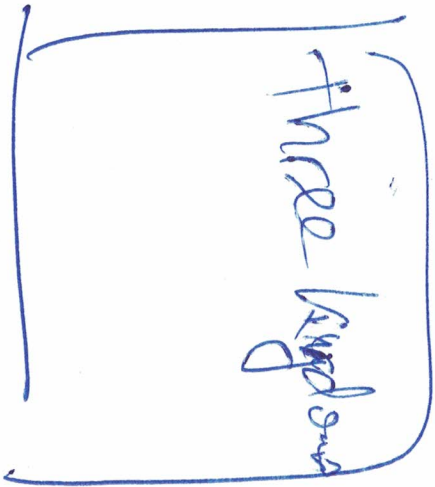
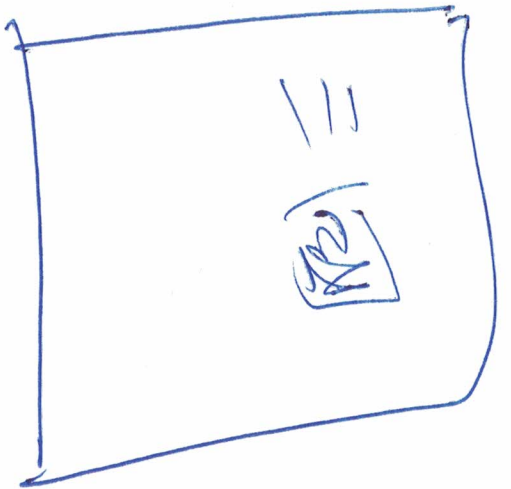
challenge:

YOO:

abababababab

your brother:

abababababab



Covert channel.