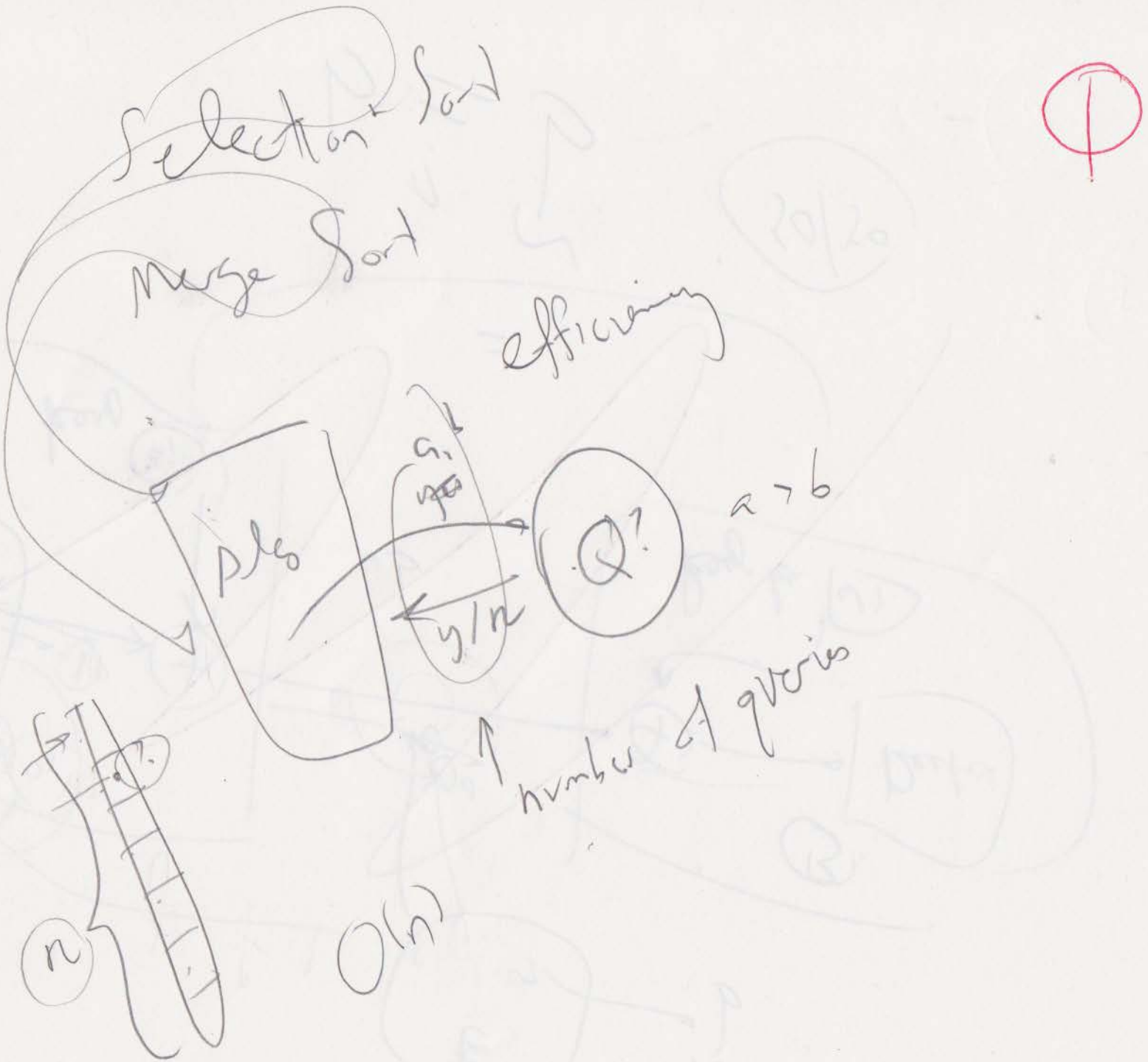
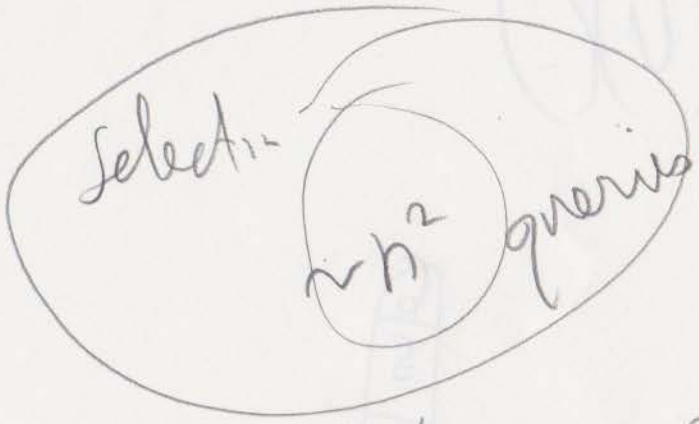
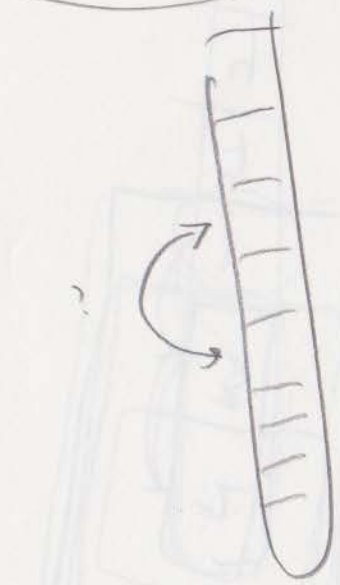
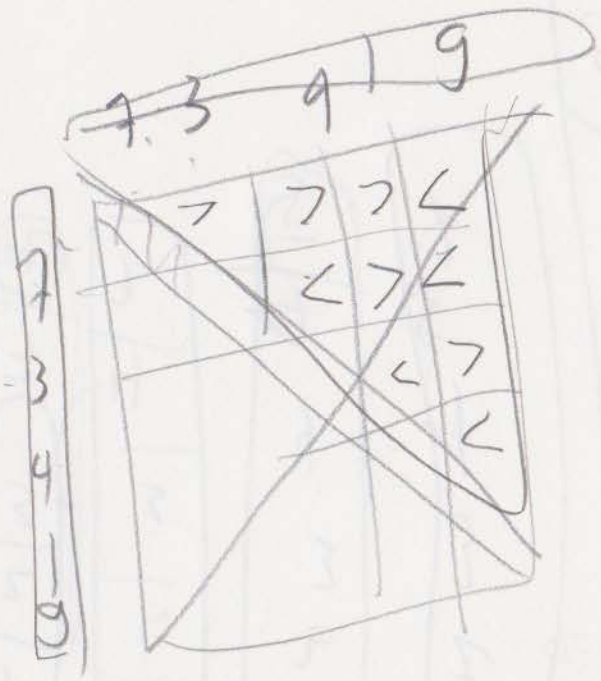

Selection Sort
Merge Sort
efficiency
Alg
Q?
a > b
y/n
number of queries
n
O(n)

at least n queries for n numbers

(2)

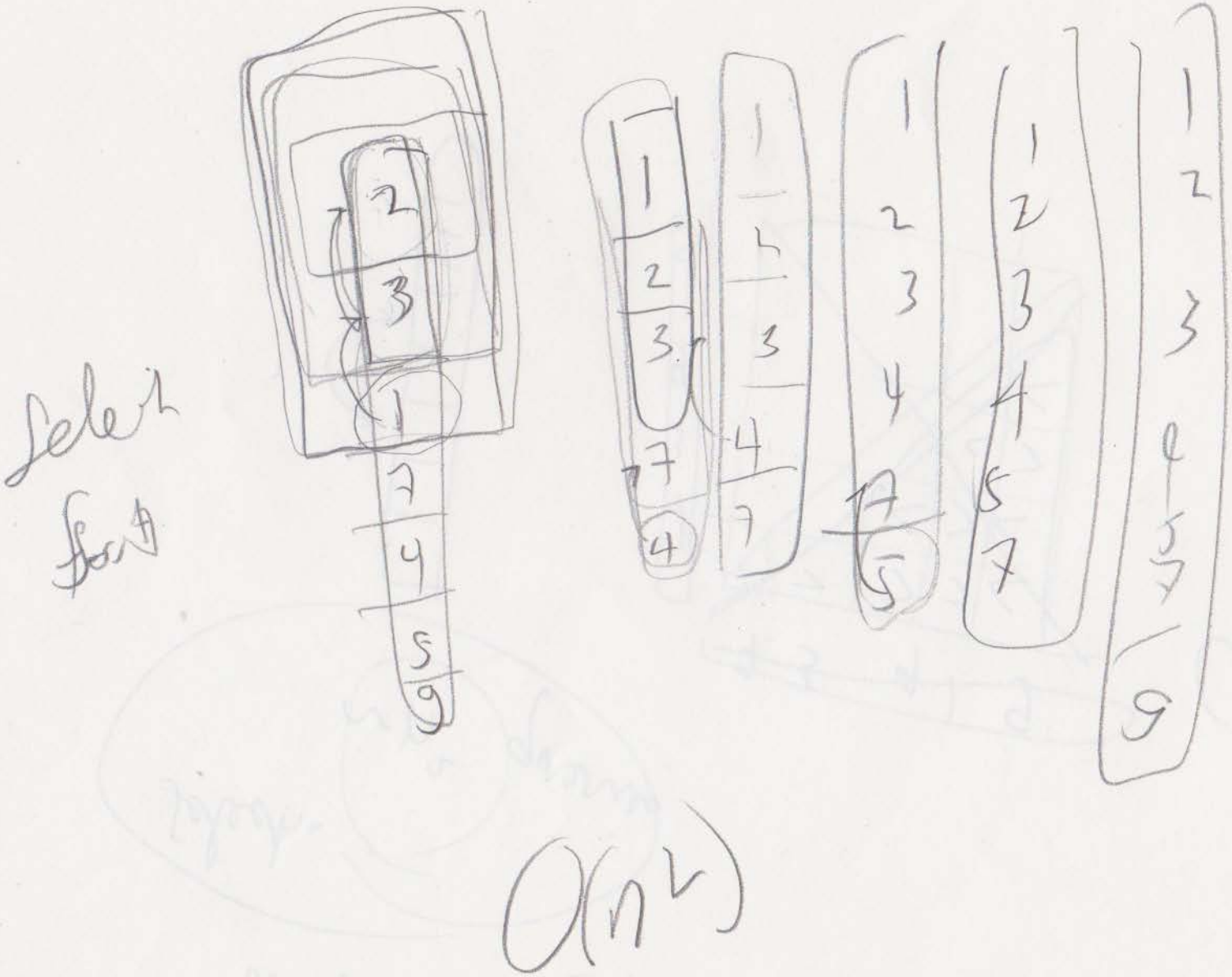






$O(n^2)$

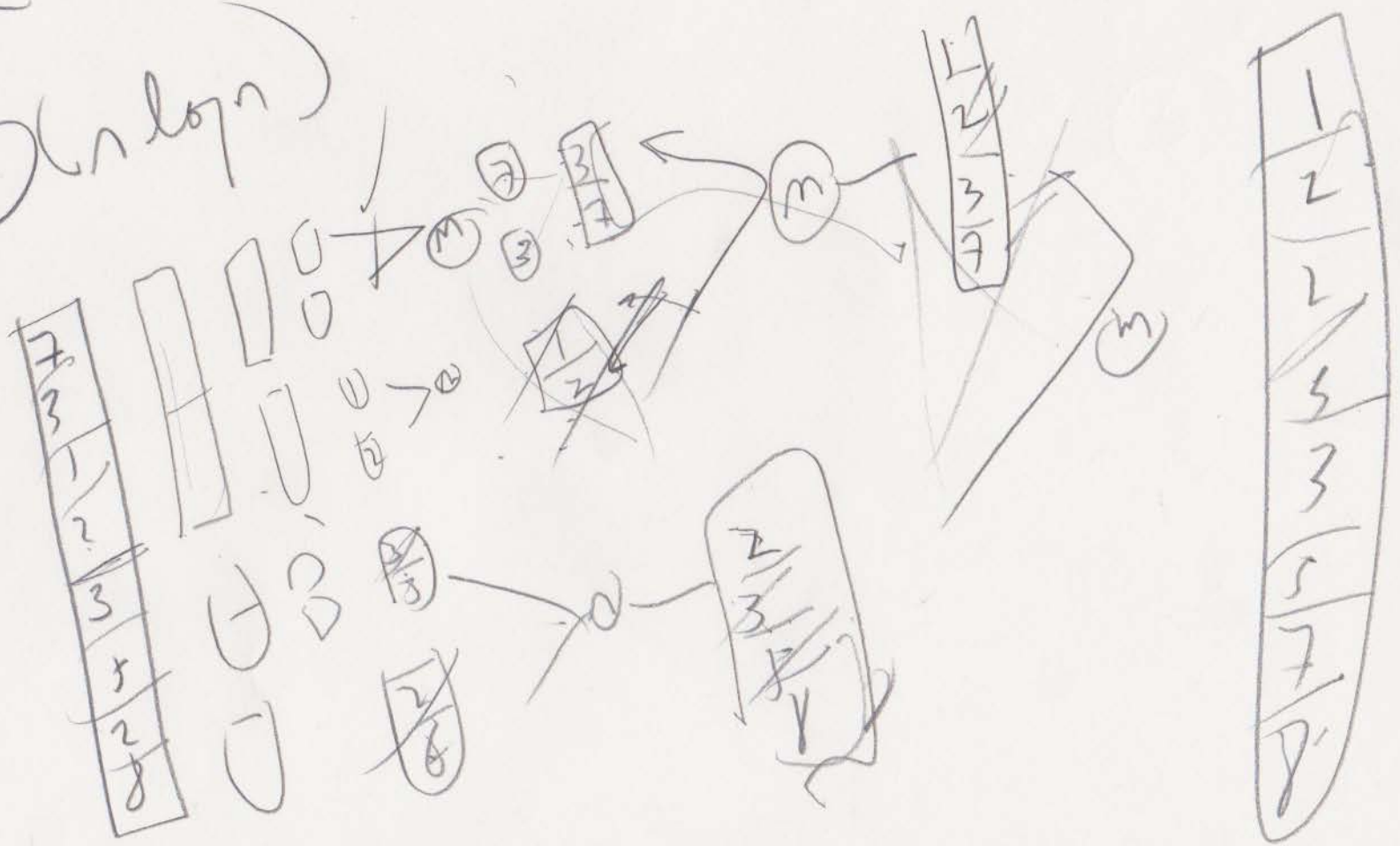
(3)

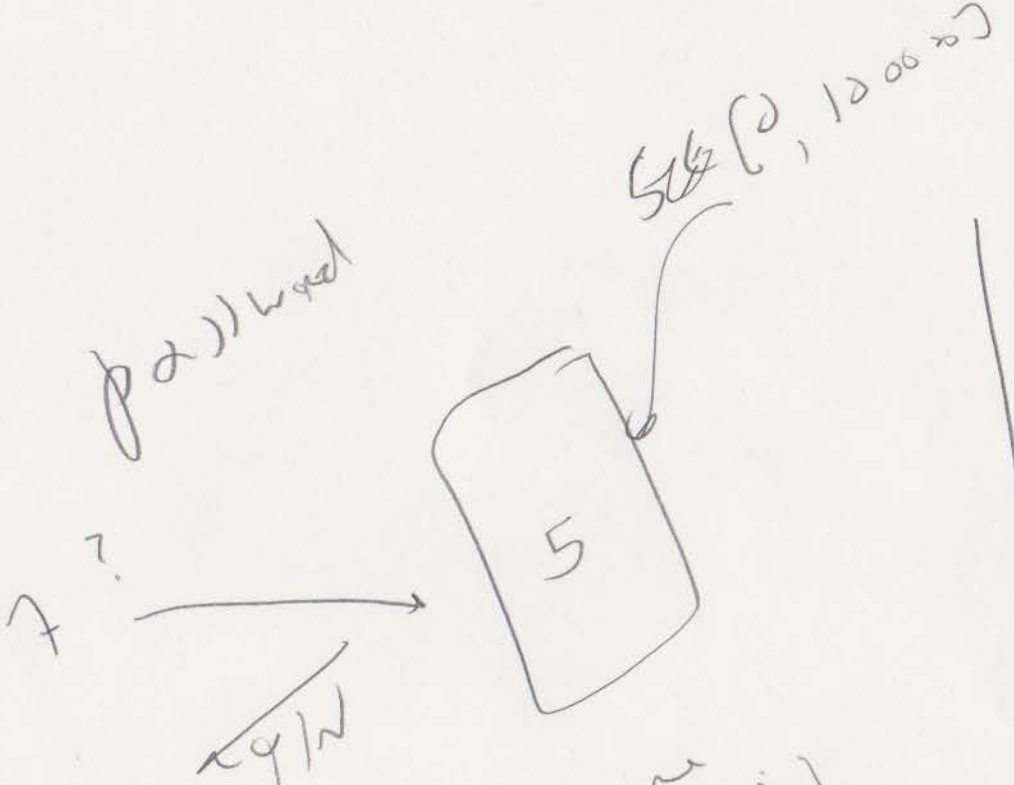


$O(n^2)$

merge sort

O(n log n)





(5)

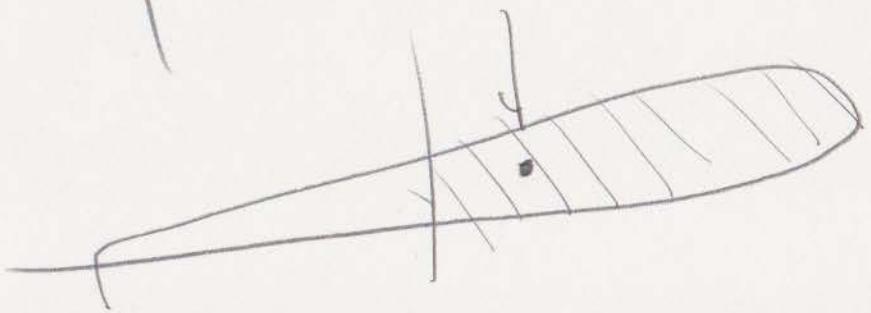
given a random

k bits

2^n password

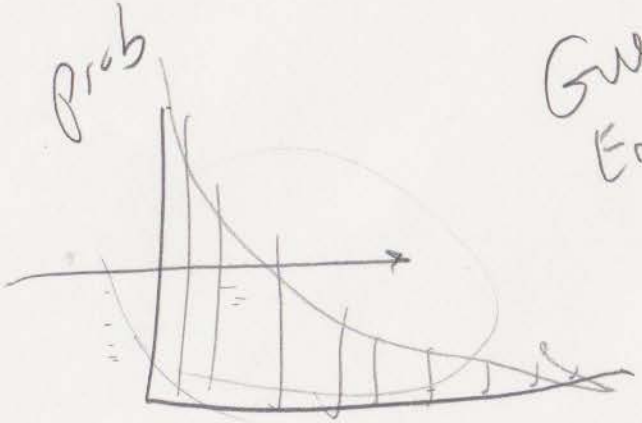
$\frac{1}{2^n}$ any given is correct

$\sim \frac{1}{2}\left(\frac{1}{2^n}\right)$ 50% you win



most likely first

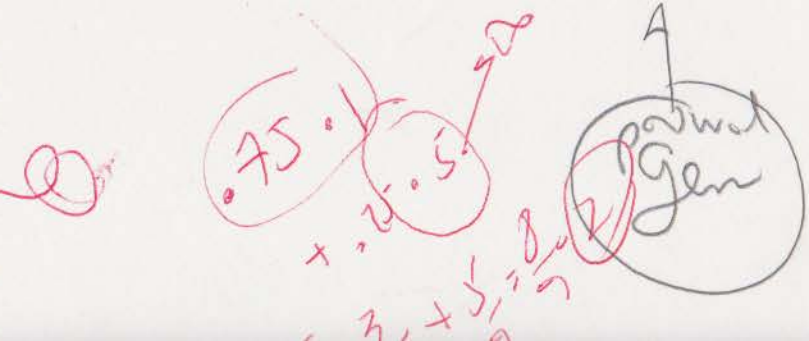
some pass words are more likely

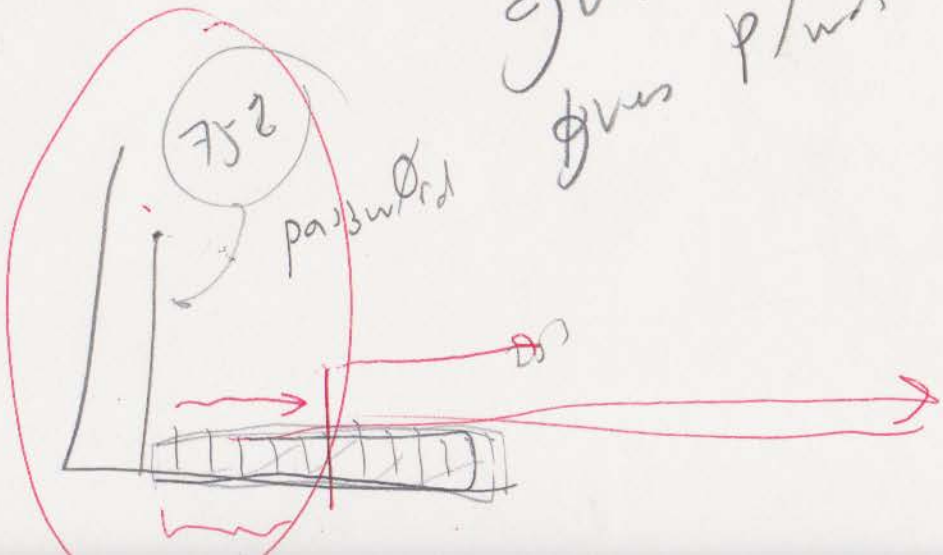


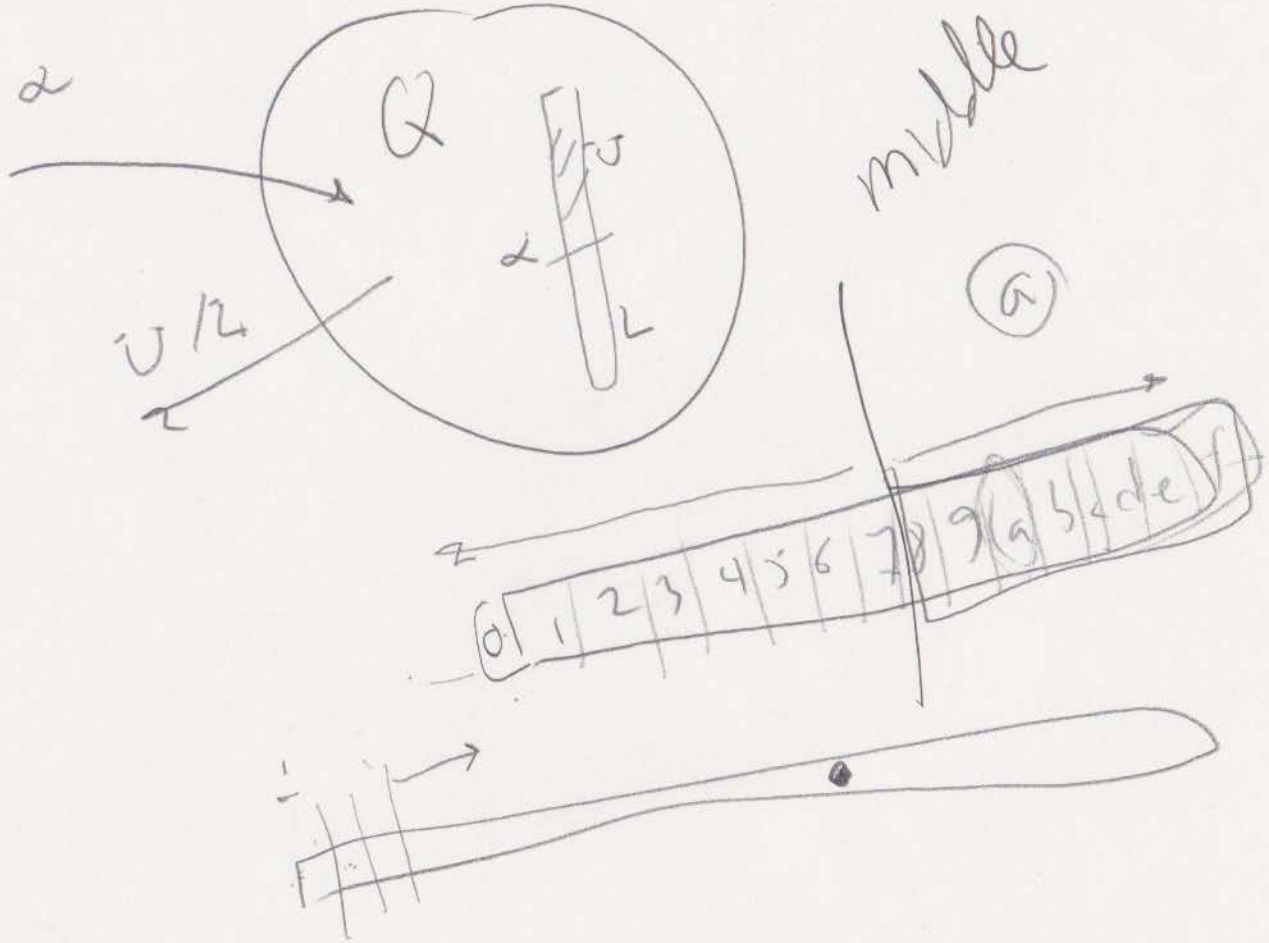
Guess Entr

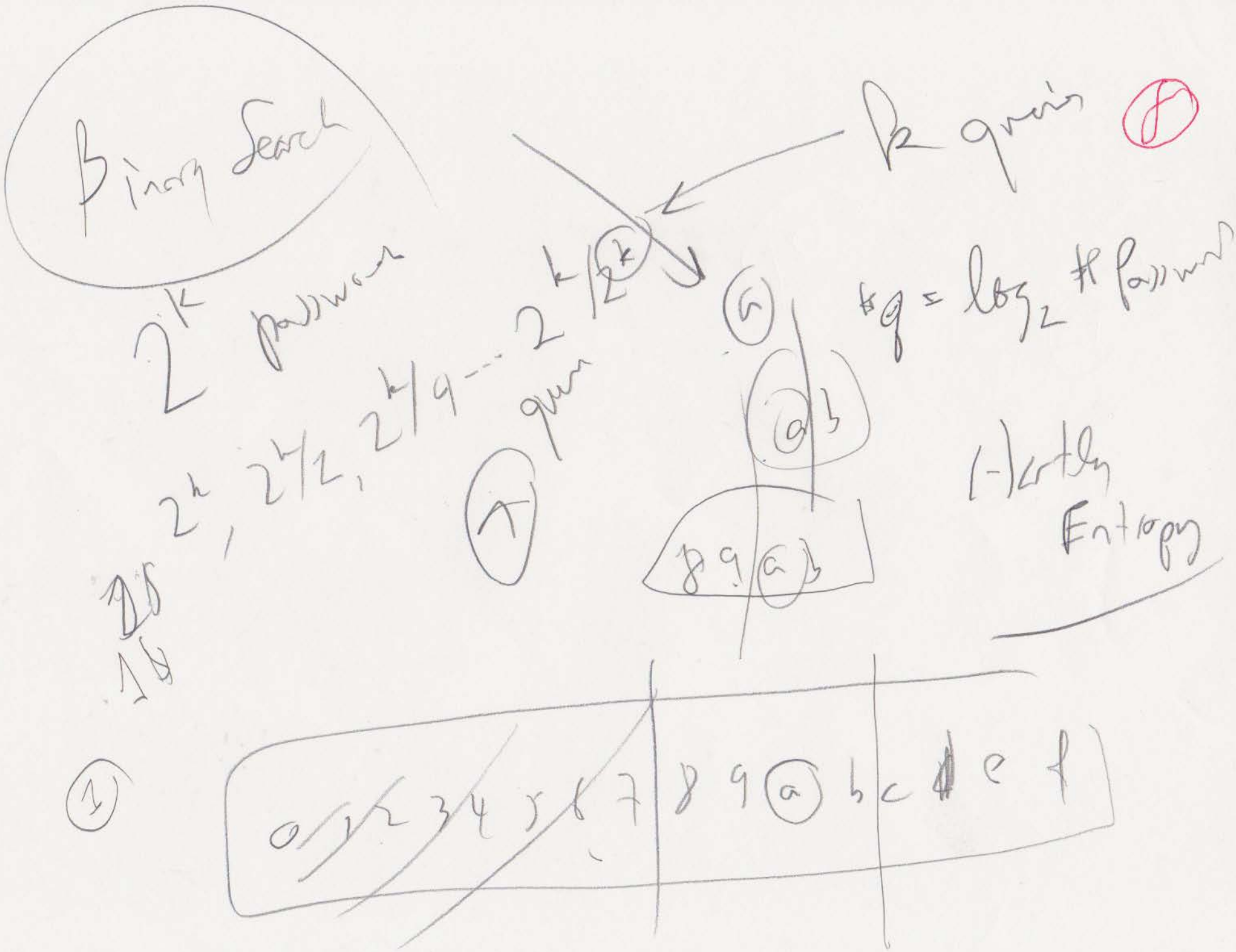
$$\sum_{i=0}^{K} p_i \cdot (i+1)$$

Expected # guess initial guess p/word






Q
v
L
U/2
milieu
0 1 2 3 4 5 6 7 8 9 a b c d e f

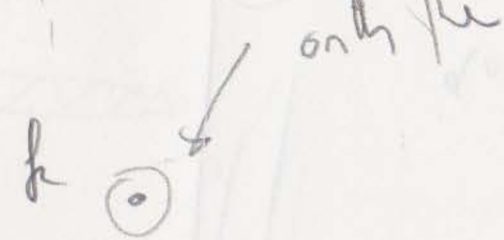

Binary Search
k queries
8
2^k passwords
$2^k, 2^k/2, 2^k/4 \cdots 2^k/2^k$
k queries
7
6
5
$\#q = \log_2 \#$ passwords
4
3
Entropy
2
1
0 1 2 3 4 5 6 7 8 9 a b c d e f

$$Hq = \text{shannon entropy}$$

$$-\sum_{i=0}^{k} p_i \log_2 p_i$$

bits

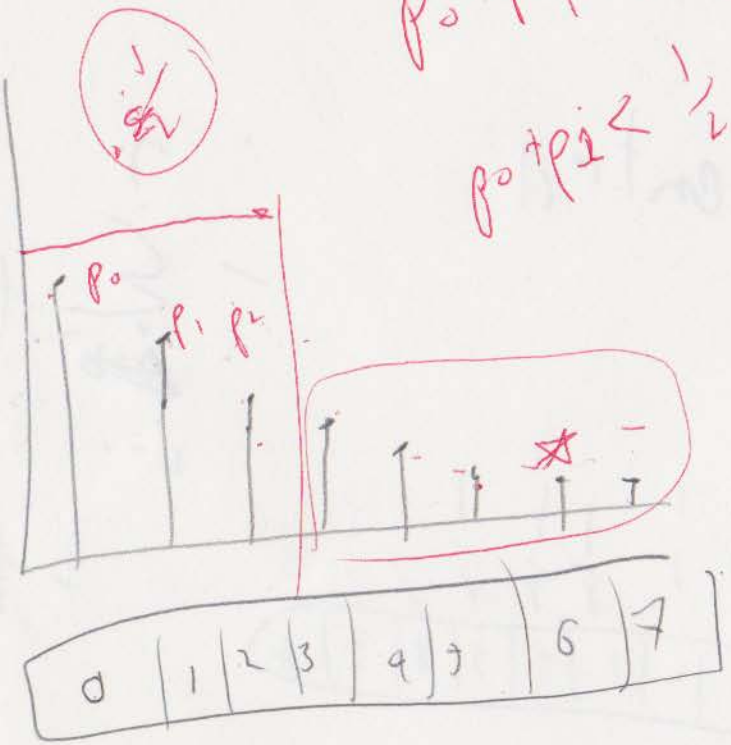
Shannon entropy



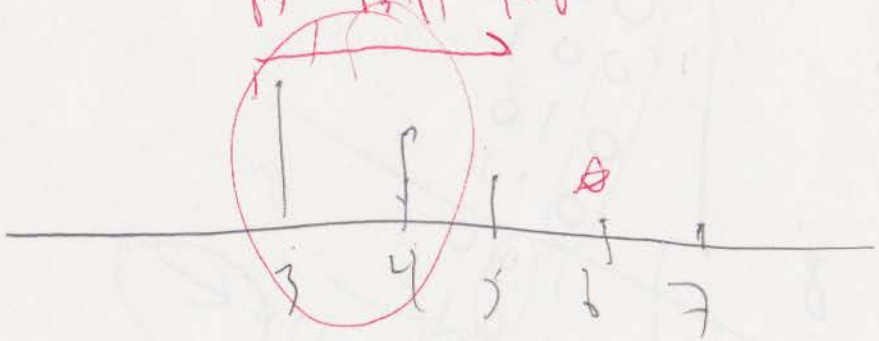
$$E(k) = -\sum p_i \log_2 p_i$$

$p_0 + p_1 + p_2 \geq 1/2$

$p_0 + p_1 < 1/2$



$p_3 + p_4 + p_5 \approx p'/2$



5/12

higher entropy

$$-\sum_{i=0}^{7} p_i \log_2 p_i$$

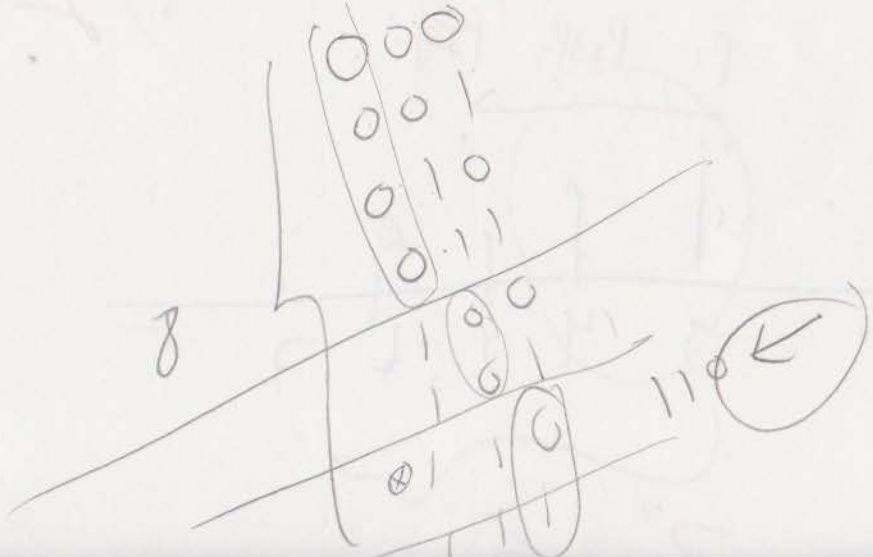
$$= \frac{1}{8} - \sum \frac{1}{8} \log \frac{1}{8}$$

$$= -\frac{1}{8}\left(\sum_{i=0}^{7}(-3)\right)$$

$$= -\left(\frac{1}{8}\right)(-3 \to 3+3 \cdots)$$

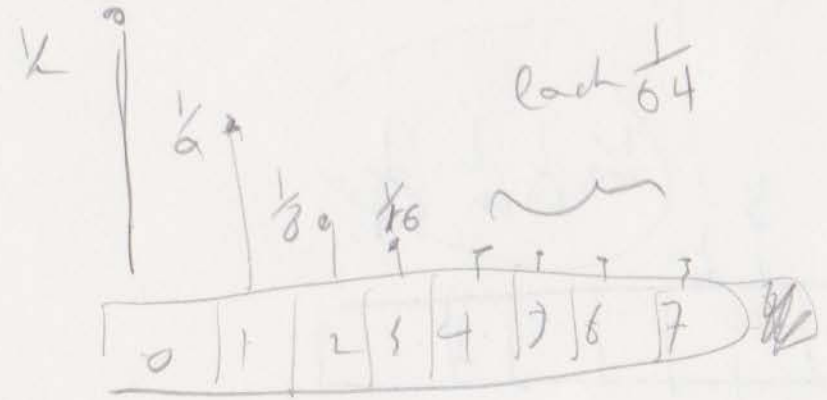
$$= +\frac{1}{8}(8(-3))$$

$$= 3 \text{ Bits}$$



Example

$H(x) = 2 \Sigma$



$p_0 = 1/2$

$p_1 = 1/4$

$p_2 = 1/8$

$p_3 = 1/16$

$p_4 = p_5 = p_6 = p_7 = 1/64$