Pls check if correct

# Question 1

A i Hash(x) = 1ms

Worst case N = 10^3

Time in worst case 10^3 ms = 1 sec

ii) worst case 10^100 ms = 3.171×10^89 years

Average case (10^10 + 10^100) / 2 ms = 1.585×10^89 years

iii) 10^56 ms for 1 entry \* 100000 entries = 10^61 ms = 3.171×10^50 years

iv)

Knowing the standard mechanism is being used (global salt concatenated at the end), it only takes 100 attempts to find the hash. This would be broken in 0.1 seconds. It would take 1.157 days to pseudonymize 100,000 records.

Hashing with a salt has much better time complexity than repeated hashing since you only call the hashing function once (all other operations assumed to be negligible). The downside is that it requires a correspondence table to reconstruct the IDs (which I guess it’s a fair price to pay not to sit for eons anonymizing a dataset).

B

i) count(dob == 11-10-1995 AND postcode == SW79TY AND dep = DoC) = 1 iff Bob is in the department, otherwise 0 (uniqueness attack)

ii) I guess you can send a million requests and it will eventually average out to 1 if he’s in the dataset, or you’ll only get 0 and TooLow otherwise?

Alternative answer: Since T has dist N(4, 2^2), it is likely at some point for the threshold T <= 0 and so the true value of the query in i) is returned. So just keep repeating the query until you get an answer which is not TooLow. If 1 Bob is in the dept otherwise he is not.

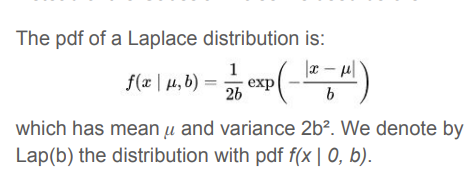
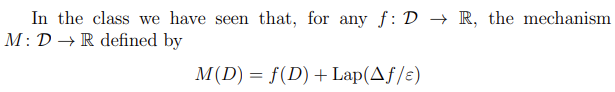
Question? Couldn’t we also use a simple intersection attack? Select everybody in the DoC and select everybody who is not born on 11-10-1995 and does not live on SW79TY. --- Yes you can but that’s not what the question is asking

C

i) D1 = [] D2 = [{id: x, grade: 20}]

sensitivity(D) = 20

ii) b = function sensitivity / epsilon = 20 / 1 = 20, variance = 2b^2 = 800

From  and maybe plus 

Iv – it is private because of the post-processing theorem.

Question 5, 6, 7 anybody??

Feel free to correct (:

v) – since M2(D)~=|D| we have that =

we can consider the noise to be the value

this gives the confidence interval as (sorry for terrible formatting)

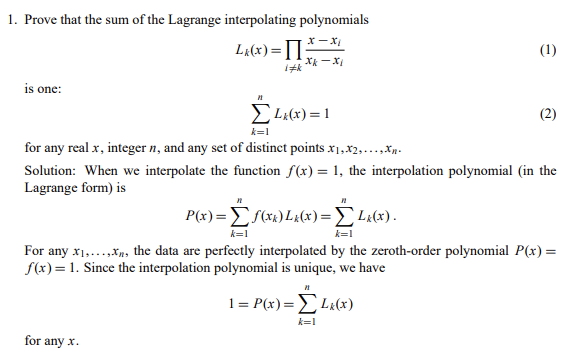
vi) – follows from v, solve for 60/eps\*|D| = 1 => |D| = 600. For privacy engineering class size 80 we get error = 7.5

vii) - see tutorial 4

# Question 2

A

From <http://sepwww.stanford.edu/sep/sergey/128A/answers4.pdf>

But use δi(x) instead of Lk(x)

B

Tutorial Question 2.7 from MPC tutorials

C

i) C1 :K1, …, KB-1 , KB+1 ,…, KN and C0 when H = B.

ii) We know A ⊕ A = 0 and A ⊕ 0 = A.

Since Bob has K1, …, KB-1 and when H = B, C0 = K0 ⊕ K1⊕ , …, ⊕ KB-1 ⊕ MB

He can do:

C0 ⊕ K1⊕ , …, ⊕ KB-1 = K0 ⊕ K1⊕ , …, ⊕ KB-1 ⊕ MB ⊕ K1⊕ , …, ⊕ KB-1

= K0 ⊕ (K1⊕ K1) ⊕, … , ⊕ (KB-1⊕ KB-1) ⊕ MB

= K0 ⊕ MB

= 0 ⊕ MB  as K0 = 0

= MB

iii) Alice cannot learn what Bob’s selection B was because it is protected by the inner 1-from-2 oblivious transfer which we can assume to satisfy the properties. This is because she cannot learn whether Bob has sent 0 or 1 and so therefore cannot determine B.

Additionally, Bob cannot learn any other messages Mi as the inner 1-from-2 oblivious transfer restricts him to learning only one of C0 or C1 at each round of the protocol. This means if he chose to learn message Mi he would not be able to learn any message Mj > I as he would be missing key Ki.