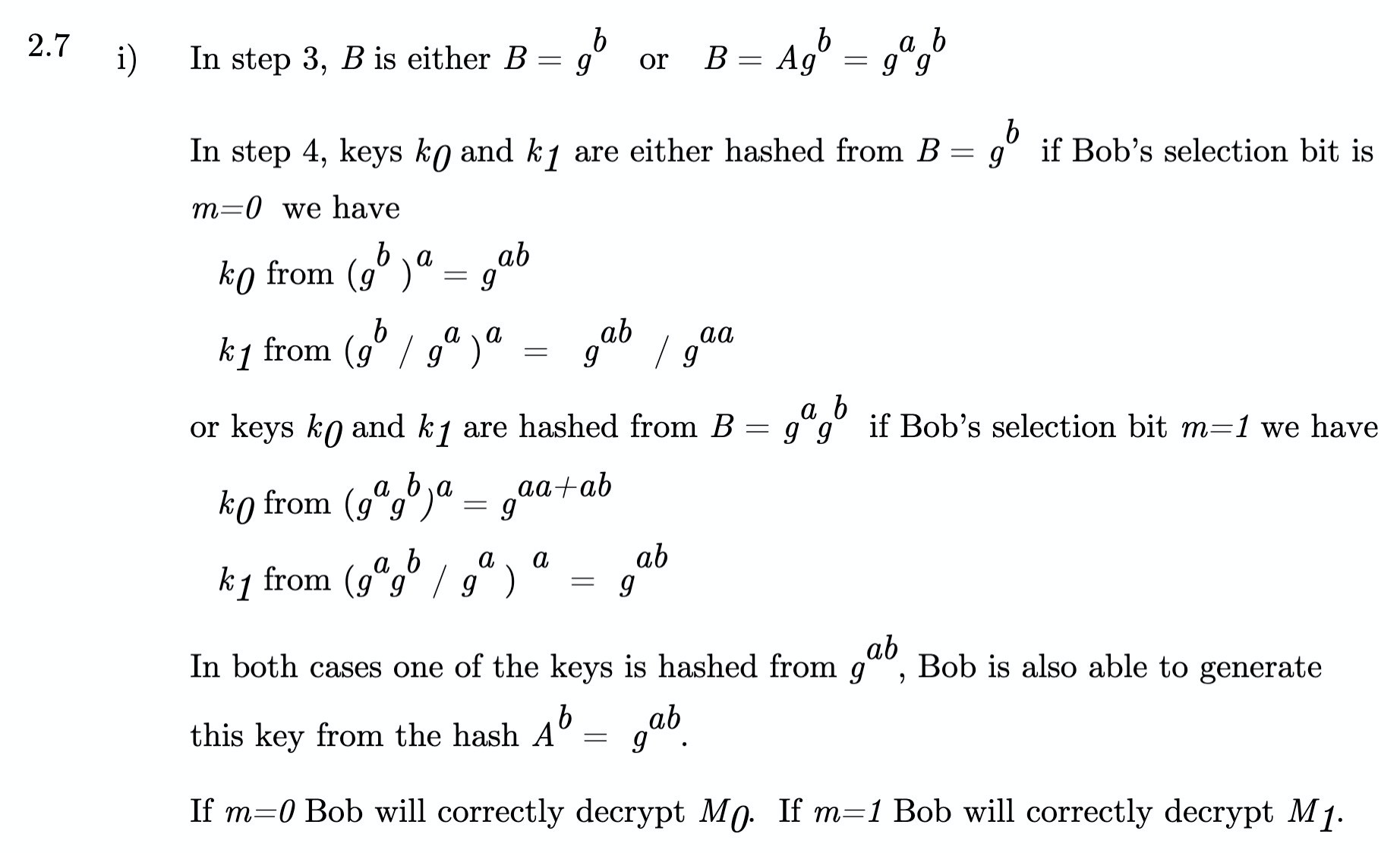
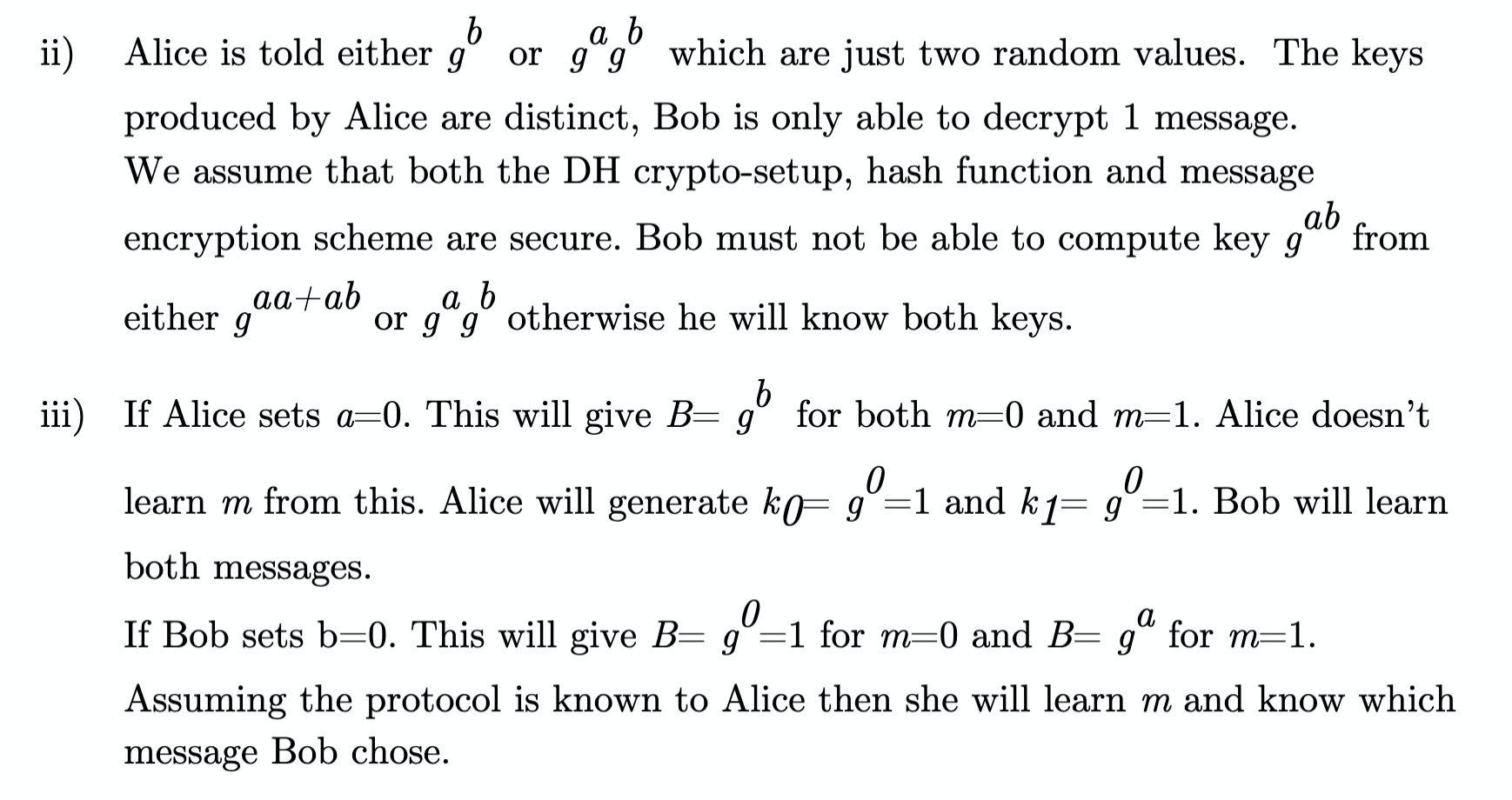
1a





1b

C\_0 = M\_0 XOR R\_b

C\_1 = M\_1 XOR R\_{1-b}

M\_m = C\_m XOR R\_t

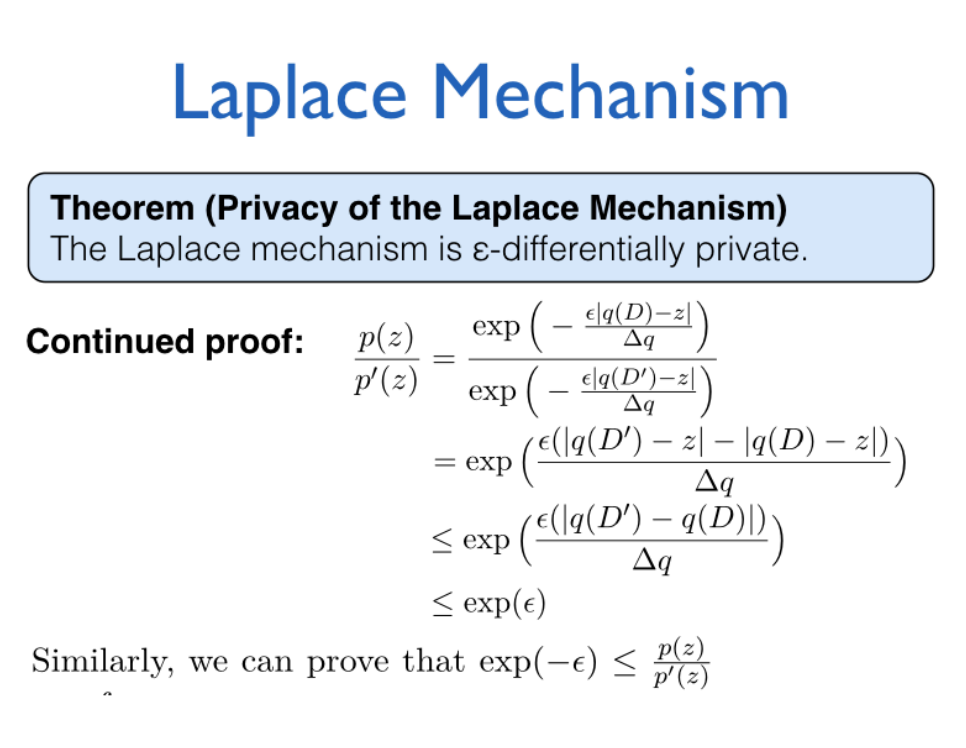
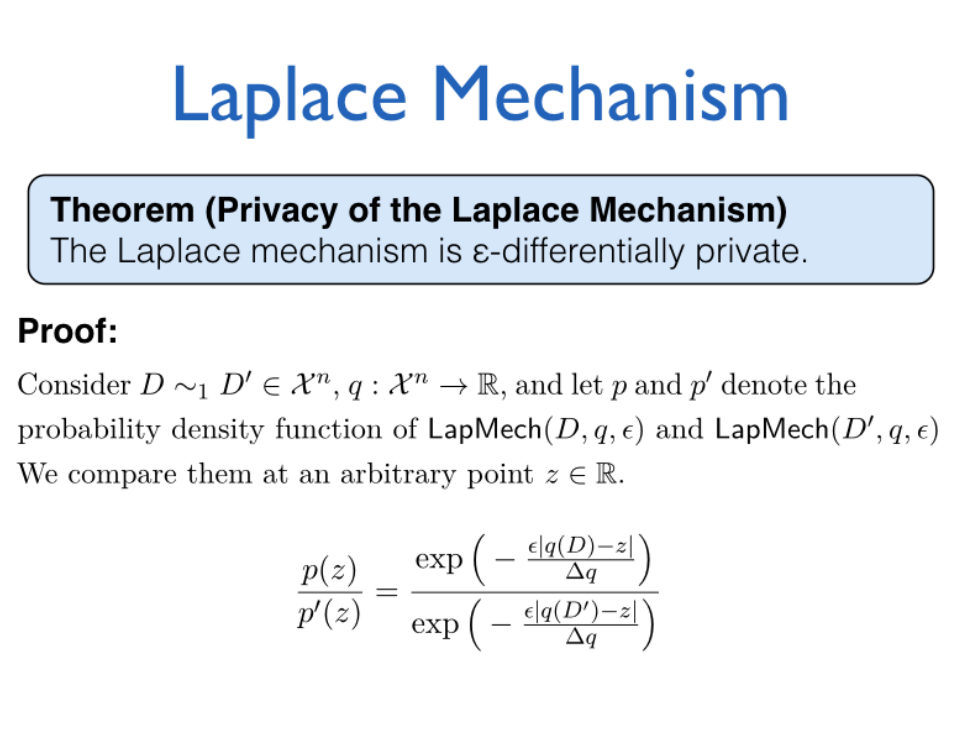
Q2 Unassessed in 2020

Q3a – I don’t think we can answer this as we don’t know what the Netflix dataset is

I think this should be along the lines of profiling attacks & averaging attacks can be performed on the dataset even if we get rid of the column names.

Q3b – I feel like this is something we should be able to do, but he never explicitly shows a proof, and when looking it up it’s a lot of stats

Stolen slides from Boston



Q3c – I mean it's just common sense, but it doesn’t really follow anything we covered, so I doubt it would be assessed

I don’t have common sense ples

Can we pls not delete the memes :’(