Privacy Engineering COMP70018=COMP97012=COMP97013 Exam feedback

Question 1: Attempting to anonymize data

Part a: Most students did very well. Some students made a mistake in subpart (i) which carried over to (ii), (iii), and (iv). We only removed the mark once.

Part b: Most students got a full mark for (i). Most also had the right idea for (ii) but some did not explain why it would work. Some tried other attacks such as intersection attacks which were not correct

Part c: This is where most students lost marks. Most students gave the correct answer to (i) although some lost marks for not properly justifying their answer. The same is true for (ii) which most students who tried received full marks for. As a result of the change in exam format, there was no (iii). Our apologies for the confusion this created.

Most students did not manage to show and justify why M' was still differentially private in (iv), often forgetting to use the post-processing theorem. Most students did not answer (v) or made a mistake in computing the confidence interval. Roughly a third of the students answered (vi) correctly with the others either not answering, making a mistake in computing the number of students, or in the CI. The differential mechanism proposed was not very good for 80 students, resulting in a large CI. Finally, not many students tried (vii), but most who did received a partial mark with some receiving a full mark.

Privacy Engineering COMP70018=COMP97012=COMP97013 Exam feedback

Question 2

Part (a) was well-answered. The hint probably helped. Some students just stated the Lagrange Interpolation Polynomial without further explanation.

Part (b) was about demonstrating knowledge of how the BGW protocol worked. Marks were lost for not showing working and not doing mod 11 calculations, otherwise answers to subparts b(i)-b(iv) applied the correct methods.

The answers to subpart b(v) were split evenly between yes/no. Quite a few reasons were given for the yes/no answers and some reasons were found in both yes/no answers! Maybe only 25% of the answers were correct.

Subparts c(i) and c(ii) were very well answered. It was pleasing to see that almost all were able to show how to recover Mb.

Subpart c(iii) was only attempted by some students, and even when it was, the explanations were often not specific to the question.