This question is bookwork and most students did very well.

Q2: Common mistakes for this question are in question C): Some students designed the protocol required in (c) to have the confidentiality requirement, which is not the case. Also anti-impersonation requires the use, and verification, of certified signature verification key, i.e. the signature verification key should be certified by a trusted CA and signature verification should include the verification of the certificate. Anti-reply requires the inclusion of timestamp in the signature. Also many students did not provide the details of signature generation and verification operations and equations.

Q3: Common mistakes for this question:
Question (a) asks about security threats in a symmetric key DISTRIBUTION process, but some students give the threats in key management in general. Question (b): In solutions provided by some students, the master key of one entity is revealed to another entity.

Q4: Common mistakes for this question:
Some students failed to associate the threats/attacks to the problem context, i.e. the answers given are too general.

Performance statistics:
In total, 117 students sat in the exam.

Question 1: taken by 103 students, and the average mark is 71%;
Question 2: taken by 103 students, and the average mark is 65%;
Question 3: taken by 57 students, and the average mark is 55%;
Question 4: taken by 91 students, and the average mark is 83%;