Question 1:
The most common mistake is in question 1(b) – could not produce correct mathematical equations.

Question 2:
The students largely did well in this question. Some lose marks due to incompleteness in answering the question. For example, in 2(b), all the process and procedures to ensure the secure distribution of public keys should be highlighted; many students failed to mention user identification/registration and certificate revocation facilities. For question 2©, some students give two PKC (public-key cryptosystem) based protocols while the question asks for one PKC-based and one symmetric-key based protocol – please note: the D-H protocol is actually a public key crypto protocol.

Question 3:
The most common mistakes were: some answers given are not really challenge-response protocols, and factors and design considerations given are not specific.

Question 4:
Generally, the students did well in this question. The common mistake is that most students fail to give any explanation of how the identified threats harm mobile customers, or only describe the threats in a rather generic context.

Some useful statistics: In total, 89 students sit in the exam.

Question 1: taken by 77 students, and the average mark is 14.5 =72%;
Question 2: taken by 88 students, and the average mark is 13.8=69%;
Question 3: taken by 32 students, and the average mark is 9.2=46%;
Question 4: taken by 69 students, and the average mark is 16.1=80%;

The overall average mark = 66.75%.
2 (out of 89 students) fail to pass the 40% mark.