Comments:

Question 1:
Some students did not do well for Question 1(b) and 1(c) – they were thinking at S-Box and permutation level!

Question 2:
Students did too well in this question, partially because the problem context is familiar to the students, I believe.

Question 3:
The most common mistakes were in (a) and (b). In (a), some students used a public key cryptosystem to design the protocol and some gave a symmetric key distribution protocol rather than a signature protocol. In (b), some students simply could not reproduce the DSA scheme.

Question 4:
The students did this question pretty well.

Some useful statistics:
---------------
In total, 73 students sit in the exam.

Question 1: taken by 65 students, and the average mark is 11.95 = 59.8%;
Question 2: taken by 67 students, and the average mark is 16.8 = 84%;
Question 3: taken by 33 students, and the average mark is 6.7 = 34%;
Question 4: taken by 53 students, and the average mark is 12.3 = 61.8%;

The overall average mark = 60%.

5 (out of 73 students) fail to pass the 40% mark; 41 (i.e. 56%) students get results >= 60%. 