Q1: The essence (thus benefit) of the challenge-response approach is to ensure that an authentication response is fresh and hard to predict. The most common mistakes are: (1) the response generated is not fresh and/or reusable, and (2) the protocols are not provided/described clearly and thoroughly.

Q2: The most common mistakes are: (1) to use an un-keyed/unprotected hash value as an authentication tag; this method cannot achieve authentication of messages that are in-transit; (2) muddle up message authentication with entity/user authentication.

Q3: This question is mostly book work and all the students should be doing well for this question.

Some useful statistics:

In total, 157 students sat in the exam.

Question 1: the average mark is 60%;
Question 2: the average mark is 73%;
Question 3: the average mark is 65%;
The overall average mark = 65.8%.

66 (out of 157=42%) students get results $\geq 70$%.
7 (out of 157=4%) failed to achieve the 40% passing mark.