Comments

Question 1:

Students did not do well in this question. The common mistakes for this question are:

- For (a), most students use the recipient's public key to encrypt the message directly. It is expensive to use a public key to encrypt long messages. You should use the hybrid encryption scheme to do this question, i.e. using the recipient’s public key to distribute a symmetric key and using the symmetric key to encrypt the long message.

- For (b), quite a few students muddle up ‘entity authentication’ with ‘message authentication’. Here the question is about message authentication. Though the two properties are connected, but only mentioning how entity authentication is achieved is not sufficient.

- For (c), quite a few students have a wrong perception that the nonces (i.e. the random numbers) should be confidentiality protected. The flaw in this protocol is that the nonce should be contributed by the verifier.

Question 2:

Students largely did well in this question.

Question 3:

Students largely did well in this question.

Question 4:

Students largely did well in this question.

Some useful statistics:

In total, 54 students sit in the exam.

Question 1: taken by 43 students, and the average mark is 8.47/20 = 42%;
Question 2: taken by 49 students, and the average mark is 14.14/20 = 70.7%;
Question 3: taken by 42 students, and the average mark is 14.28/20 = 71.4%;
Question 4: taken by 37 students, and the average mark is 14.48/20=72.4%;

The overall average mark = 64%.

6 (out of 54) failed to achieve the 50% passing mark.

35 (out of 54) students get results >= 60%.