Comments

Question 1:
This question is bookwork and you should not do badly in this question.

Question 2:
This question is also bookwork.

Question 3:
This question is an easy one, as you experience many issues covered in this question in your daily life, but, to get the full mark, your answer must be technically correct and complete.

Question 4:
This is a hard question (though it looks easy), and this is also the worst performing question. To gain the full mark on this question, one has to demonstrate thorough understanding of the authentication security property as well as its relationship with other security properties.

4(a): Many students fail to see the fact that, in a distributed system, authentication is a prerequisite for several other security services, such as message confidentiality, message integrity, authorisation and accounting, etc, etc. It is the first line of defence in any computer system.

4(b): This question asks you to identify a protocol flaw, i.e. what is the flaw in that three-step protocol. The key point here is that a nonce used in an authentication protocol must be contributed by the verifier. Also many students mix up authentication with confidentiality. Here the messages do not need the confidentiality protection – it is about authentication! All we need is for the claimant to demonstrate the knowledge of a secret to the verifier, which is the essence of entity authentication in a distributed or networked environment.

4(c): The most efficient way of implementing this protocol is to use a keyed hash function (keyed hash function takes less computational time than symmetric key encryption), and, of course, as mentioned above, the nonces should be contributed by the verifier, not the claimant.

Some useful statistics:
---------------
In total, 106 students sat in the exam.

Question 1: taken by 102 students, and the average mark is 59%;
Question 2: taken by 53 students, and the average mark is 63%;
Question 3: taken by 84 students, and the average mark is 65%;
Question 4: taken by 76 students, and the average mark is 46%;

The overall average mark = 58%.

15 (out of 106) failed to achieve the 40% passing mark.

35 (out of 106) students get results >= 70%.