Hello ... How are you? ...

Here are the questions of the Security and Monaqasat ... I hope I remember as much as I saw in the exam ... It was 20 pages of questions ... no blank pages ... no rest ... 2 hours ... so be patient while reading the questions.

CONCEPT QUESTIONS

*** Alice thinks that she has invented a protocol that makes her authenticate her peer (i.e. making sure that it's Bob who is talking to her). The protocol proceeds as follows
1- Alice generates a pseudorandom number
2- Alice ecrypts this number with a previously shared key with Bob (i.e. assume no one knows the key except Alice and Bob)
3- Alice sends the ciphertext
4- Bob receives the ciphertext
5- Bob decrypts the ciphertext using the same shared key
6- Bob encrypts the output of step (5) using the same encryption key
7- Bob sends the output of step (6) to Alice
8- Alice receives this then decrypts using the same shared key
9- If Alice found the output of (8) the same number generated in (1), then It's true that Bob is the peer of Alice. Else, It's not Bob who is communicating with Alice.

The question is :D Is there an error in this protocol and if ther is can you modify it to fix this error?

CHAPTER 1