50.005 Quiz NS 2 (15 mins)
Name: _**Sample Solutions**_____________ Student ID: ________________

Note: During the quiz, you can consult written or printed materials. But you can't go online or look at anything electronic, including your laptop, smartphone, etc.

1. In RSA, suppose we have a public key (n=55, e=3). Find the private key (n,d) corresponding to the public key such that d is the smallest possible.

(n=55, d=27) [3pt].

Note: p=5; q=11; z=40. Need 3d mod 40 to give a remainder of 1; smallest 3d is 81, so d is 27.

2. What is a nonce? Explain why the use of a nonce in an authentication protocol can help defend against the playback attack.

A nonce is an identifier that is guaranteed to be fresh (i.e., never used before) [2pt]. Because a nonce is fresh, whoever replies to it must also be fresh and can't be a previously recorded version of the replier [2pt].

3. Assume that Alice and Bob had previously established a secret symmetric key S for encryption of communication between them, and Alice obtained a message M from Bob encrypted by S. For each of the following statements, say if it is true or false and explain why.

a) Alice knows that the message must indeed have come from Bob.

True [1pt]. Only Alice and Bob are able to generate the message, and Alice knows that she didn't do it [2pt].

NB: The intended meaning of "come from Bob" is that Bob authored the message. If student answers false and explains it by saying that someone else may have sent Bob's message to Alice, count the answer as correct.

b) Alice can take the encrypted message to court with non-repudiation that the message indeed came from Bob.

False [1pt]. Since besides Bob, Alice could also have generated the message, she can't prove it to the court that the message came from Bob and not her [2pt].