

CMSC 417 Homework uhm, Four

Due Tuesday, May 13. 1PM, so that I can check that I've received it before class. TURNIN PROCEDURE: Turn in this homework as a TEXT FILE encrypted for me:

```
2989 7EB7 2B2B 9256 A9B1 66AE B6F8 5756 FB90 DE84
```

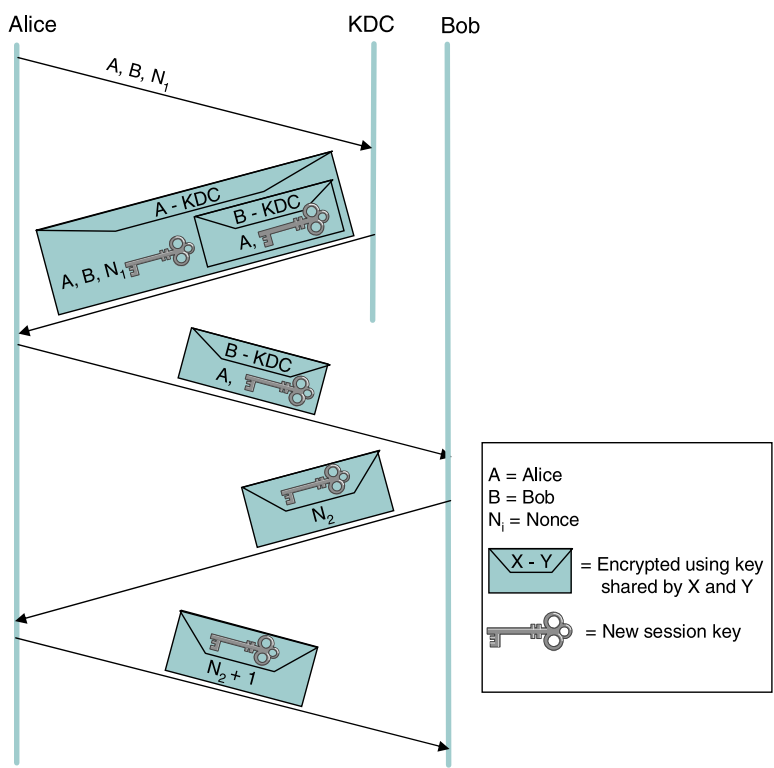
key id FB90DE84.

```
gpg --keyserver pgp.mit.edu --search-keys nspring
```

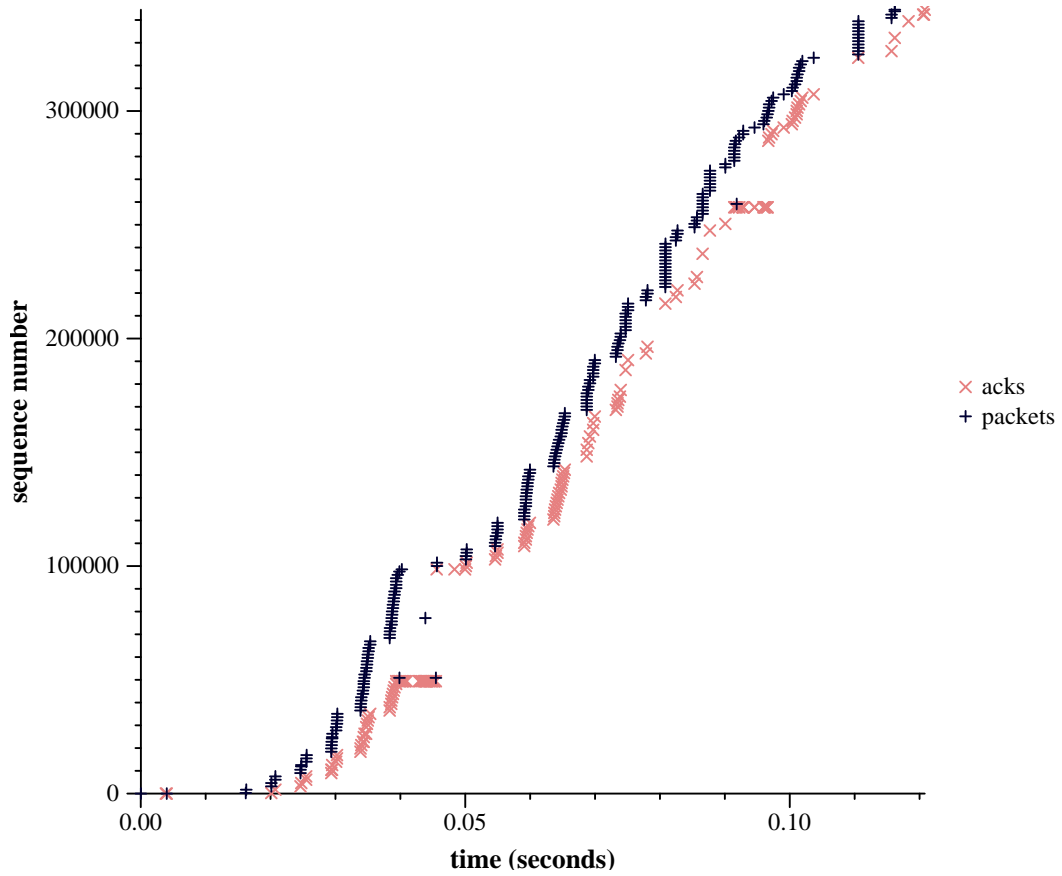
You may use whatever facilities are in your email client, use a different email client, or attach a file that is the encrypted version of the text file. You may sign the homework as well (optional). If I can't recover it, you'll have to show me the process for decryption (which means, you might want to test that you can decrypt things you encrypt to yourself before turning something in.)

Of course, I'll hand off the decrypted versions to Bo, so please include your name inside the text file.

No, it is not an ideal mechanism for secure turn in of homework. Thankfully, if someone else tries to spoof homework for you either it's good (you didn't do it) or it's obvious (two turn ins).



1. Page 634 exercise 4 (which is the following). In the Needham Schroeder protocol above, the question is, if an adversary can eavesdrop the messages and eventually discover the Alice-Bob key, what does the adversary have to do to trick Bob into a conversation as if the adversary is Alice?



2. In the following sequence/ack plot, (a) how did the sender know (or decide) to transmit only the packet at sequence number 77,147, time 0.0438? (and not the packets immediately before and after it.). (b) what do you estimate the RTT to be? (c) was the second retransmission of 50,867 necessary? (d) what was the largest window?

3. Why won't reverse path filtering stop spoofing?