CS3235 tutorial questions for the days of (Mon Oct 18-Fri Oct 22, 2004) (Not sure what week...)

October 16, 2004

I gave a wrong answer for Q5 in the MCQ. There are two correct answers. I will correct my mistake sometime soon, and update the marks. Thanks for your correction.

1. (Textbook, p94) RESEARCH: What is Clipper key escrow? Briefly describe the Clipper chip and key escrow.

2. The Needham Schroeder protocol to share a key K can be described as follows:

Alice	$\rightarrow$	Charles	:	{Alice,Bob,n_1}
Charles	$\rightarrow$	Alice	:	{Alice,Bob,n_1,K,{Alice,K}k_{Bob}}k_{Alice}
Alice	$\rightarrow$	Bob	:	{Alice,K}k_{Bob}
Bob	$\rightarrow$	Alice	:	$\{n_2\}K$
Alice	$\rightarrow$	Bob	:	$\{n_2 - 1\}K$

In this protocol description, A$\rightarrow$B:X means A sends message X to B, n_1 and n_2 are randomly generated numbers, $\{X\}K$ means encrypt X using session key K, and $\{X\}k_{\text{Attila}}$ means encrypt X using Attila's private key.

(a) Two of the participants must trust the third participant. Which participant is the one that two others MUST trust?

(b) Which participant generates the session key K to be shared between the other participant?

(c) Why does Alice calculate $n_2 - 1$?

(d) Are the last two messages needed? If YES, why? If NO, why not?

3. In the protocol described in question 2, we assume that the session key K is secure. Outline what could go wrong with the protocol if hacker Harry could *discover* a session key K. Outline how you could fix this problem.

4. In the contract signing protocol outlined in the lecture, as time goes on each party has less and less reason to break off the contract early. Why is this?

5. (Textbook, p94) Design, or discover a contract signing protocol, which uses a third party to oversee the contract.