CS3235 Tutorial for week 12
(Oct 27th-Oct 31st, 2003)

24th October 2003

1. In Windows 2000 and XP, Microsoft introduced a Kerberos-based authentication scheme to provide more secure authentication over a network. Unfortunately, in most networks using Windows 2000 and XP, passwords/hashes can still be retrieved from the network. Why is this?

2. The buffer overflow attack described in class seems like it should be *fixable*.

(a) Outline steps you might take to ensure that a program you had written did not suffer from a buffer overflow attack.

(b) Given that the attack is well known amongst programmers, why are there so many attacks?

3. Buffer overflow attacks in general might be fixable by making changes to the Operating System. Make at least two suggestions as to how the buffer overflow attack may be limited by making changes to the OS.

4. Secure shell uses RSA for authentication. What does it use for encryption?

5. In the picture of the *pgpfone* preferences dialog, there is a button labelled CAST. What is CAST?