CS3235 Tutorial for week 11
(Oct 20th-Oct 24th, 2003)

18th October 2003

1. **Question 8, Chapter 12 in textbook:** Does using passwords with salts make attacking a specific account more difficult than using passwords without salts? Explain why or why not.

2. **Question 1, Chapter 13 in textbook:** The postscript language describes page layout for printers. Among its features is the ability to request that the interpreter execute commands on the host system.

   (a) Describe a danger that this feature presents when the language interpreter is running with administrative or *root* privileges.

   (b) Explain how the principle of least privilege could be used to ameliorate this danger.

3. **Question 2, Chapter 13 in textbook:** A common technique for inhibiting password guessing is to disable an account after three consecutive failed login attempts.

   (a) Discuss how this technique might prevent legitimate users from accessing the system. Why is this action a violation of the principle of least common mechanism?

4. Alice is sending a message to Bob using RSA encryption. Bob chooses intital values $p = 71$, $q = 97$, and $E = 41$

   (a) Calculate x and N and Bob's public key N, E.

   (b) Calculate D and Bob's private key N, D.

   (c) If Alice wanted to encode "Hi", she might use the ascii values as integers: "H" in decimal is the integer 72. "i" in decimal is the integer 105. What value messages does Alice transmit to Bob?

   (d) What calculation does Bob perform to retrieve the orignal messages?

   (e) Harry-the-hacker has a difficult problem. What is Harry's difficult problem?