CS3235 Tutorial for week 3
(Aug 25-Aug 29, 2003)

25th August 2003

1. **Notes, Chapter 1, question 2:** Differentiate between a Cæsar cipher and a Vigenère cipher.

2. **Notes, Chapter 1, question 3:** In his column "Why cannot?" in Streats, June 19, 2003, Geoffrey Pereira was annoyed that he had to key ctrl-alt-del to bring up the password prompt. He discovered how to bypass this sequence to save time, and this will be replicated to the 800 or so other employees of his company. Geoffrey seemed to miss discovering a specific reason for this mode of operation, and by bypassing the key sequence, he opens his company to a particular kind of attack. Discover the *reason*, and the *attack*.

3. In class, we looked at a three-way system for transferring a message from A to B, which had the interesting property that neither A nor B had to reveal their keys. Given a message m, the first message (from A to B) would be $K_A(m)$, the second message (from B to A) would be $K_B(K_A(m))$, and the third message (from A to B) would be $K_A^{-1}(K_B(K_A(m))) = K_B(m)$. B could then calculate $K_B^{-1}(K_b(m)) = m$, and retrieve the message. If both A to B used a random byte sequence for their key, and then used the XOR function to both encrypt and decrypt the message, then surely this is a perfect technique for transferring data... right? (Neither participant has to reveal a key, and a third party cannot decrypt/unlock the message).
   Well... actually... it is not a good scheme. Explain exactly why it is not a good scheme.

4. **Notes, Chapter 2, question 5:** Given a bit string a, show how to use another *mask* bit string m of the same length to reverse a fixed bit position i, that is, change 0 to 1 and 1 to 0, but just in position i.

5. **Notes, Chapter 2, question 6:** How many bits are needed to represent a number that is 100 decimal digits long? How many decimal digits are needed to represent a number that is 1000 bits long? How many decimal digits are needed to represent a number that is 100 decimal digits long?