COSC244 Tutorial
From Lecture 8 & 9

1. Distinguish between encryption and decryption.

2. Distinguish between ciphertext and plaintext.

3. What is a Caesar cipher?

4. What is a poly-alphabetic cipher? How do you decrypt the cipher text?

5. If the encryption key is long enough, encryption techniques such as bit level ciphering are truly unbreakable. Why don't they use more bits as the key?

6. What is the Data Encryption Standard (DES)?

7. The following was encrypted using a Caesar cipher. What is the original message?

   fcvceqoowpkecvkqpucpfeqorwvgtpgvyqtmu

8. Given the bit string 00101 10101 01000 01111 11010 01101 and the key 10110, use the key to encrypt the string using bit-level ciphering.

9. Given the encrypted bit string 01101 10101 01010 01111 11010 01111 and the key 10110, use the key to decrypt the bit string to recover the original data.

10. Use the transposition cipher with 5 columns to encrypt the following text: Data communication is a very interesting paper. Read the text in the order of columns 3 5 1 4 2.

11. What are some problems with non-public key encryption systems?

12. How does public key encryption differ from regular encryption?

13. What is a digital signature? Using a digital signature, how do you determine whether a message is sent by the sender if he denies sending the message?

14. What are the main features of the RSA algorithm?

15. What makes the RSA algorithm so difficult to break?

16. Explain the process used when one wants to share a file that can be authenticated. That is, we want to be sure the file was not altered. An example would be a software patch from a company such as Microsoft.