CSS 322 – QUIZ 1

Last name: _____   First name: _____

ID: _____   Total Marks: _____
                                                                                                out of 13

- Write your name and ID in the space provided at the top of the sheet.

- Answer the questions on this sheet(s) only, using the space given.

Question 1 [3 marks]

a) Sakol wants to send Anick a message. Write the name of the security service that is needed for each of the following cases:

   a. Anick wants to be certain that the message came from Sakol, and not from Adikan.   Service:_____

   b. Anick wants to be certain that Adikan has not changed the original message sent by Sakol.   Service:_____

   c. Sakol wants to be certain that Adikan cannot read the message.
                                                                        Service:_____

b) If Adikan performs the following actions, then indicate if it is a Passive or Active attack (circle the correct answer):

   a. Adikan captures the message, and at a later time, sends it again to Anick.
                                                                        PASSIVE or ACTIVE

   b. Adikan captures the message, and makes observations about how Sakol and Adikan are communicating.   PASSIVE or ACTIVE

   c. Adikan pretends to be Sakol, sending a message to Anick.
                                                                        PASSIVE or ACTIVE

Question 2 [3 marks]

Indicate whether each statement is True or False (circle the correct answer):

a) Analysis of frequency of letters to break a cipher can only be applied if the plaintext language is English.   T / F

b) The Vigenere cipher is an example of a polyalphabetic cipher.   T / F

c) Steganography has an advantage over cryptography if you don't want someone to know who you are sending a secret message to.   T / F

d) The ciphertext produced by the Vigenere cipher cannot be attacked by analysing the frequency of single letters.   T / F

e) Although unconditionally secure, the one-time pad is not practical because a ciphertext can be decrypted to multiple legible (understandable) plaintext messages with different keys.   T / F

f) Using substitution operations are more secure than transposition operations in symmetric key ciphers.   T / F

Question 3 [4 marks]

    a) Assume you have a modified Caesar Cipher where the alphabet contains the digits 0 to 9 (instead of the letters A to Z). Write an equation that defines the encryption process of this cipher if the plaintext digit p maps to the ciphertext digit C when key k is used.

        Equation:

    b) In the cipher in part (a), how many possible keys are there? _____

Question 4 [3 marks]

A Transposition Cipher (but not a Rail-fence Cipher) was used to produce the following ciphertext:

        UO!HZESSSQTYTIOIIA

The key used was: 5 2 6 3 4 1

What was the plaintext used (it is in English)?

Plaintext: _____