Information Security Technologies COMP607
Tutorial

Session 1 – Introduction and classical ciphers
Introduction:

1. Which of these situations would require protection for CIA?

	C	I	A
Exam question file sent by email for printing	□	□	□
Exam results posted on notice board	□	□	□
Letter from your employer:	□	□	□
about your payrise	□	□	□
about your promotion	□	□	□
about new staff joining	□	□	□
A file in your computer storing your passwords	□	□	□
Online newspaper report	□	□	□

2. Give some examples where Kerchoffs’s principle is (i) applied, (ii) not applied

3. What is them main requirement for the key according to Kerchoffs’s principle?

4. Encrypt the following message “`ENEMY PLANE SPOTTED`” using:

   (a). Ceasar's cipher,
   (b). Vignere cipher using key: `SUNSHINE`

   Use (i) graphical method, (ii) numerical method

5. Decrypt the following cipher text using the Vigene table, and key : `HANGZHOU`

   `IEGZDY ZUAE GNZU BYCEE`

6. Decrypt the following ciphertext which was encrypted using rail fence cipher with key =3.

   `EYIEYVRDYSNWAEAAD`

7. Encrypt the following using the rail fence cipher with key=4

   `THERE IS NO SUCH THING AS A FREE LUNCH`

8. *We received the following ciphertext which was encoded with a shift cipher:
`xultpaajcxitltlxaarpjhtiwtgxktghidhipxciwtvgtpilpitghlxiwiwtxgqadds`

   (a). Perform an attack against the cipher based on a letter frequency count: How many letters do you have to identify through a frequency count to recover the key? What is the cleartext?

   (b). Who wrote this message?