Information Security
Information & Network Security
Classwork 4 - Solutions

David Weston
DCSIS, Birkbeck, University of London

This classwork is *not* marked. All classworks and their solutions will be made available online.

1. Consider the following cipher texts

   (a) AHAH

   (b) ABCD

   (c) ZQRZ

   (d) ARAWR

   Which, if any, of the cipher texts could result from encrypting the word FEET using any monoalphabetic substitution cipher? Explain your answer.
   Solution:
   A monoalphabetic substitution cipher maps each letter of the alphabet onto a permutation of that alphabet. From this definition we can deduce the following properties:
   1) The length of the ciphertext must equal the length of the message.
   2) The number of unique letters in the message must equal the number of unique letters in the ciphertext.
   3) Repeated letters in the message must correspond to repeated letters in the ciphertext.
   The message, FEET, is 4 characters long and has 3 unique characters and a repeated letter in the middle. All of these properties must exist in the cipher text.
   Hence, none of the candidate cipher texts are possible.

2. Using the playfair cipher, encrypt the word:
   hello
   with the key:
   information

Solution:

i	n	f	o	r
m	a	t	b	c
d	e	g	h	k
l	p	q	s	u
v	w	x	y	z

hello has a repeated character, so we need to insert an x:
he lx lo
now we can encrypt, the cipher text is:
kg qv si