CSS322 – Quiz 2

Name: ______________________ ID: ______________ Marks: _____ (10)

Question 1 [2.5 marks]

Consider a mono-alphabetic cipher, with a selected mapping from plaintext to ciphertext for all possible plaintext values shown below (the mapping is split into two to fit it on the page).

```
p: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z a
C: V W O Q R C P m f e g H q Z S t h F z r w Y c y D o -

p: b c d e f g h i j k l m n o p q r s t u v w x y z _ -
C: l L u _ E K s B A v n G N i T b k X p M j I U a J x d
```

(a) With a computer that can make 10^{12} decrypt attempts per second, what is the worst case time for a brute force attack? [1.5 mark]

(b) Explain a practical attack against the cipher. [1 mark]

Question 2 [3 marks]

(a) ________________________ is a security service that assures the received data originated from the claimed sender.

(b) In a ________________________ attack, a malicious user sends an identical copy of a previous message they have intercepted.

(c) The information known only to sender and receiver in a cipher is called a ________________________

Question 3 [2 marks]

Using the first 8 letters of your full name (convert all uppercase to lowercase, and delete any characters which are not letters a—z) as a keywords, encrypt the ciphertext *polls* using the Playfair cipher.

Plaintext: ______________________________

Ciphertext: ______________________________

Question 4 [2.5 marks]

Consider the ciphertext `fsxbosrrlteweixuco` output from a rows/columns transposition cipher using the key `236451`. What is the plaintext?

Plaintext: ______________________________