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 b
C: _ D g f i J T e z v w Q L G N d c b O ! l y R o M n H V

p: 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: x Z k E j u q C p K r F h B A X I P Y ? t S W U # a s m
```

(a) With a computer that can make 10^{10} 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 controls who can have access to a resource.

(b) The process of converting a coded message back to the original message is called _____.

(c) In a _____ attack, a malicious user observes patterns of communications, without having to read the message contents.

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 *muddy* using the Playfair cipher.

Plaintext: _____

Ciphertext: _____

Question 4 [2.5 marks]

Consider the ciphertext `cieaexshxettrbxass` output from a rows/columns transposition cipher using the key `164325`. What is the plaintext?

Plaintext: _____