

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 10^9 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) In a _____ attack, a malicious user overloads a server or network with traffic.

(b) _____ is a security service that assures data received are exactly as sent.

(c) The process of converting an original message into a coded, apparently random message is called _____.

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 *merry* using the Playfair cipher.

Plaintext: _____

Ciphertext: _____

Question 4 [2.5 marks]

Consider the ciphertext `sthseeteitaxabrdsenx` output from a rows/columns transposition cipher using the key 42135. What is the plaintext?

Plaintext: _____