

CSS322 – Quiz 1

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

For reference, you may use the following mapping of English characters to numbers:

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 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 |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Question 1 [3 marks]

Consider the ciphertext `tgnhogitxktxywxorxnixiuo` output from a rows/columns transposition cipher using the key 81237456. What is the plaintext?

Question 2 [3 marks]

- (a) Name an attack that the data confidentiality service aims to prevent. Describe how the attack works.

- (b) Explain the difference between a passive and active attack.

Question 3 [4 marks]

Consider a Vigenère cipher where the alphabet is the first ten letters from the English alphabet, i.e. a to j .

- (a) Encrypt the plaintext **feed** with keyword **bed**. What is the ciphertext?

- (b) If a computer took 1ms to perform one decryption, on average how long would a brute force attack take on this cipher?