

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 [2 marks]

Encrypt the first 3 letters of your firstname using the Vigenère cipher with the keyword *hello*.

Question 2 [5 marks]

Fill in the blanks.

- In a _____ attack, a malicious user overloads a server or network with traffic.
- _____ is a security service that assures data received are exactly as sent.
- The process of converting an original message into a coded, apparently random message is called _____.
- Consider a One Time Pad that uses octal (base-8) digits, as opposed to English letters. A computer system can decrypt this One Time Pad at a rate of 10^7 messages per second. In theory, the average time to apply a brute force attack on this One Time Pad when a message is 200 characters is _____ seconds. [2 marks]

Question 3 [3 marks]

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