CSS322 - Quiz 1

Name:								ID:									_ Marks: (1									
	F	or	· re	efe	rer	ıce	э, у	σu	ım	nay	use	the	foll	lowi	ng 1	map	pin	g of	En	glisl	h ch	ıara	cter	s to	numbe	ers:
						_			_						_	_								у 24		

Question 1 [3 marks]

Consider the ciphertext httessoatxtsseaumeoxeubexiihnyqnvox output from a rows/columns transposition cipher using the key 3162745. What is the plaintext?

Question 2 [3 marks]

(a) Name an attack that the availability 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 high 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?