

# 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 [4 marks]

You have access to a computer that can perform  $10^{10}$  decryption operations every second. What is the average time it would take you to find the plaintext for a given ciphertext when using the following cipher: Monoalphabetic substitution cipher. Assume each cipher uses the 26 letters from the English alphabet (although keywords, if used, also use these letters, they do not have to be a known English word or phrase). Assume each decryption operation also includes a check as to whether the plaintext is correct or not (and such a check always works).

## Question 2 [2 marks]

What is the main reason a polyalphabetic cipher (such as Vigenère) offers stronger security than a monoalphabetic substitution cipher?

**Question 3** [4 marks]

Encrypt the plaintext **steven** with a Vigenère cipher using the keyword **crypto**.