CSS322 – Quiz 1

Name: ____

ID: ______________________________ Mark: __________ (out of 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 [2.5 marks]

The Thai alphabet has 76 characters (ignoring special characters and punctuation). Assume a modified Caesar cipher was created to operate on the Thai alphabet.

a) Write an equation the describes the encryption operation of the Thai-based Caesar cipher, assuming a plaintext character *p*, key *k* and ciphertext character *c*. [1.5 marks]

b) How many possible keys are there for the Thai-based Caesar cipher? [1 mark]

Question 2 [2.5 marks]

Encrypt the first 8 characters of your name using a Vigenere cipher and the key SIIT. Start with your first name, and if it is less than 8 characters continue with your second name, ignore spaces (for example, I would encrypt: “stevengo”). Write your final answer here:

___ ___ ___ ___ ___ ___ ___ ___

Question 3 [3 marks]

Consider a system with two normal users Apiwat and Benjarak, and a malicious user Chinorot. The following statements describe *either* a security service required by the normal users *or* an attack performed by the malicious user. If the statement describes a service, then give the name of the service. If the statement describes an attack, give the name of the attack.

a) Benjarak wants to be certain that the message came from Apiwat, and not from Chinorot.

Service *or* attack: ___________________________

b) Chinorot obtains a copy of a message sent from Apiwat to Benjarak, and Chinorot tell's his friends about the message contents.

Service *or* attack: ___________________________

c) Chinorot sends many messages to Benjarak so that her computer is too busy to receive messages from Apiwat.

Service *or* attack: ___________________________

Question 4 [2 marks]

Assume I designed my own cipher to encrypt exam answers. The cipher uses a 40 bit key. I always create the answers 10 days before the exam and store them on my office computer, however on the same day that I created the exam answers a malicious student obtained access to my office computer and took a copy of the answers. The malicious student has free access to a computer that can decrypt the answers at a rate of 200×10^9 attempts per day (as the student wants to cheat on the exam, they don't know about any limitations in the encryption algorithm). Is this system used for encrypting exams computationally secure? Explain your answer, showing any calculations where necessary.

(Note that $2^{10} \approx 10^3$, $2^{20} \approx 10^6$, $2^{30} \approx 10^9$, and so on)