CSS 322 – QUIZ 1 ANSWERS

First name: ______________________________ Last name: ___________________________

ID: _____________________________ Total Marks: ____________

out of 10

Question 1 [3 marks]

a) Jirapath wants to send Nuttakorn a message. Write the name of the security service that is needed for each of the following cases:

a. Nuttakorn wants to be certain that the message came from Jirapath, and not from Benjawan.

Service: AUTHENTICATION

b. Jirapath wants to be certain that Benjawan cannot read the message.

Service: CONFIDENTIALITY

c. Nuttakorn wants to be certain that Benjawan has not changed the original message sent by Jirapath.

Service: INTEGRITY

b) If Benjawan performs the following actions, then indicate if it is a Passive or Active attack (circle the correct answer):

a. Benjawan captures the message, and at a later time, sends it again to Nuttakorn.
ACTIVE

b. Benjawan captures the message, and makes observations about how Jirapath and Nuttakorn are communicating. PASSIVE

c. Benjawan pretends to be Jirapath, sending a message to Nuttakorn.
ACTIVE

Question 2 [3 marks]

a) Assume you have a modified Caesar Cipher where the alphabet contains the digits 0 to 9 (instead of the letters A to Z). Write an equation that defines the encryption process of this cipher if the plaintext digit *p* maps to the ciphertext digit *C* when key *k* is used.

Equation:

E(p) = (C + k) mod (10)

b) In the cipher in part (a), how many possible keys are there? 10

Question 3 [4 marks]

A rows and column Transposition Cipher was used to produce the following 30 element ciphertext:

VYCAPODEYYEIUNTITGICSNRDOLUSTR

You have managed to discover the last 3 elements of a 6 element key: __ __ __ 1 3 5

What was the plaintext used (it is an English sentence)? Show your calculations below.

Plaintext: I LOVE STUDYING SECURITY AND CRYPTO

Calculations:

Since there are 30 characters and 6 character key, then five rows:

VYCAP ODEYY EIUNT ITGIC SNRDO LUSTR

1 2 3 4 5 6

We know the last three columns:

V	E	S
Y	I	N
C	U	R
A	N	D
P	T	O

Trial and error can be used to discover the first three columns. The first 3 letters can be:

OIL VES – unlikely (although OIL is a word, it is unlikely start of sentence

OLI VES – possible (OLIVES …)

IOL VES – not a recognisable word

ILO VES – possible (I LOVE S…)

LIO VES – not a recognisable word

LOI VES – not a recognisable word

Therefore trying the two possible options (OLI = 2 6 4 or ILO = 4 6 2)

2	6	4	1	3	5
O	L	I	V	E	S
D	U	T	Y	I	N
E	S	G	C	U	R
Y	T	I	A	N	D
Y	R	C	P	T	O

4	6	2	1	3	5
I	L	O	V	E	S
T	U	D	Y	I	N
G	S	E	C	U	R
I	T	Y	A	N	D
C	R	Y	P	T	O

Therefore the key is 4 6 2 1 3 5.