CSS 322 – QUIZ 1 ANSWERS

First name: _____ Last name: _____

ID: _____ Total Marks: _____

out of 10

Question 1 [4 marks]

Warrapat wants to send Chavalit a message.

a) Write the name of the security service that is needed for each of the following cases:

   a. Chavalit wants to be certain that the message came from Warrapat, and not from Sarissa.

      Service: Authentication_____

   b. Warrapat wants to be certain that, after receiving the message, Chavalit does not deny that he received it.

      Service: Non-repudiation_____

Warrapat sends a message to Chavalit.

b) If Sarissa performs the following actions, then indicate the type (or name) of attack *and* indicate if it is a Passive or Active attack (circle the correct answer):

   a. Sarissa sends many messages to Chavalit, so that he can no longer uses his network connection.

      Type: Denial of service_____ **Active** / Passive

   b. Sarissa captures the message, makes a change to the message, and at a later time, sends the changed message to Chavalit.

      Type: Modification_____ **Active** / Passive

   c. Sarissa captures the message, and makes observations about how Warrapat and Chavalit are communicating.

      Type: Traffic analysis_____ Active / **Passive**

Question 2 [2 marks]

Describe two disadvantages of using steganography to hide a secret message.

Answer

The technique relies on the attacker not knowing the algorithm. Once the attacker discovers the algorithm, all past and future messages can be deciphered.

It is often inefficient. A large fake message must be sent in order to communicate a small real message.

Question 3 [2 marks]

Encrypt the message “This quiz is easy” using the Vigenere cipher and the key SIIT. Treat all characters as the same case, ignore spaces, and use the mapping shown on this page.

S	I	I	T											
18	8	8	19											
P		T	h	i	s	q	u	i	z	i	s	e	a	s	y
		19	7	8	18	16	20	8	25	8	18	4	0	18	24
		18	8	8	19	18	8	8	19	18	8	8	19	18	8
		11	15	16	11	8	2	16	18	0	0	12	19	10	6
C		l	p	q	l	i	c	q	s	a	a	m	t	k	g

Question 4 [2 marks]

The following ciphertext was encrypted using a rail fence transposition cipher. What is the original plaintext? There were no padding (extra) characters needed or used when encryption occurred.

Ciphertext: ndooaoywudbksroonyeg

Answer

As there was no padding used, then it means the depth of the fence is either 1, 2, 4, 5, 10 or 20. Depths of 1 or 20 produce a ciphertext no different from plaintext. Hence, you could first try a depth of 2 to see if there is a corresponding English plaintext. Then try a depth of 4. It turns out a depth of 4 produces:

n	d	o	o	a
o	y	w	u	d
b	k	s	r	o
o	n	y	e	g

The plaintext is: Nobody knows youre a dog.