Uva Wellassa University of Sri Lanka
Faculty of Applied Sciences
Department of Computer Science Informatics
300 Level 1st Semester Examination – Jul. /Aug. 2019
CST333-2 Data and Network Security

Uva Wellassa University

Instructions to candidates

This paper consists of two (02) parts: Part A (Structured), and part B (Essay).

Duration: Two (02) hours

Total mark allocation: 100

Answer all the questions

Do not remove this question paper from the examination hall.

Part A

Number of questions: Six (06)

Mark allocation: 30

Index Number:

1.

a. Differentiate vulnerability and attack. (3 mark)

.....

.....

.....

.....

.....

.....

.....

b. List the categories of threats. (2 mark)

.....

.....

.....

.....

2.

a. Specify five (05) categories of OSI security services. (2.5 mark)

.....

.....

.....

.....

.....

b. What is cryptanalysis? (1.5 mark)

.....

.....

.....

.....

.....

3.

a. What is meant by diffusion? (2 mark)

.....

.....

.....

.....

.....

.....

b. What is the purpose of S-box in DES algorithm? (2 mark)

.....

.....

.....

.....

4.

a. Fill in the blanks with most appropriate words. (3 mark)

i. Rail Fence is an example of ..... .

ii. In the DES algorithm the round key length is ..... bits and the Round Input is ..... bits.

iii. Triple DES use ..... or ..... number of keys.

iv. AES-256 perform ..... number of rounds.

b. What are the three (03) security goals achieve in digital signature? (3 mark)

.....

.....

.....

.....

5.

a. Mention two (02) issues in security for which Public Key Cryptography developed to address. (2 mark)

.....

.....

.....

.....

b. Specify four (04) public key distribution mechanisms used in cryptography. (4 mark)

.....

.....

.....

.....

.....

6.

a. What are the five (05) principle services provided by Pretty Good Privacy (PGP)? (2.5 mark)

.....

.....

.....

.....

b. Why does PGP generate a signature before applying compression? (2.5 mark)

.....

.....

.....

.....

.....