The Open University of Sri Lanka
Faculty of Natural Sciences
B.Sc/ B. Ed Degree Programme

Department	**: Computer Science**
Level	**: Five**
Name of the Examination	**: Final Examination**
Course Title and - Code	**: CSU5309 – Information Security and Cryptography**
Academic Year	**: 2019/2020**
Date	**: 20.10.2020**
Time	**: 1.30 pm – 3.30 pm**
Duration	**: 02 Hours**

General Instructions

1. Read all instructions carefully before answering the questions.
2. This question paper consists of **06** questions in **03** pages.
3. Answer any **04** questions only. All questions carry equal marks.
4. Answer for each question should commence from a new page.
5. Draw fully labelled diagrams where necessary.
6. Involvement in any activity that is considered as an exam offense will lead to punishment
7. Use blue or black ink to answer the questions.
8. Clearly state your index number in your answer script

Q1.

(i) What is Computer Security?

(ii) Briefly describe why systems must keep records of their activities.

(iii) Describe the components of Security Systems Development Life Cycle.

(iv) Briefly describe the following terms related to protection mechanisms

a. Protection Domain

b. Trusted Computing Base

c. Abstraction

d. Rings

e. Reference Monitor

Q2.

(i) What are the two Key Management mechanisms used with IPSec security association establishment?

(ii) Describe the secure coding mechanisms that can be used in following cases;

a. Buffer overflows

b. Code Injection

(iii) Describe about two attacks that bypass OS security.

(iv) Discuss how the security gets effected by the ethical differences across cultures.

Q3.

(i) What is a Key Table? Describe how it is created and its uses.

(ii) Draw a block diagram to describe the function of Triple DES.

(iii) Describe the use of mixing algorithm and salt in PBE (Password Based Encryption)?

(iv) Write the steps of the encryption and decryption of bulk data using PBE.

Q4.

(i) What are the mechanisms we can use to share a key in symmetric key cryptosystems and discuss their problems?

(ii) What is digital envelope? Describe the process.

(iii) What are the five (05) areas considered in evaluating cryptographic algorithms?

(iv) Discuss the mechanisms used for protecting private key in PKC.

Q5.

(i) What is digital signature? Describe the use of digital signature.

(ii) Briefly describe how HMAC works with help of a diagram.

(iii) Describe the function of RSA.

(iv) Describe about the digital certificate.

Q6.

(i) "Public key cryptography gives you not only a powerful mechanism for encryption but also a way to identify and authenticate other individuals and devices. But one drawback is the integrity and ownership of a public key." Discuss the statement.

(ii) Briefly describe about the entities collaborated in PKI (Public Key Infrastructure)?

(iii) What are the trusted models used in PKI? Draw diagrams.

(iv) Name and briefly describe the mechanisms used to safeguard and limit access to private keys.

*****End of Examination Paper*****