THE OPEN UNIVERSITY OF SRI LANKA

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE

B. SC. DEGREE PROGRAMME 2017/2018

FINAL EXAMINATION

CSU5309: INFORMATION SECURITY AND CRYPTOGRAPHY

DURATION: TWO HOURS (2 HOURS)

Date: 25.03.2019 **Time: 1.30 pm – 3.30 pm**

Answer **FOUR** Questions **ONLY.** All questions carry equal marks.

Q1.

(i) What are the three (03) essential components of security?

(ii) Distinguish between security service and security mechanism using example Services/ Mechanisms.

(iii) Briefly describe following goals of security:

a. Authorization

b. Integrity

c. Availability

d. Authenticity

e. Non-repudiation

(iv) The following is a list of cryptographic types as well as methods. Organize them in a logical tree structure.

Pubic Key Encryption, Private Key Encryption, Asymmetric Key Encryption, Symmetric Key Encryption, DES, AES, Stream Ciphers, Block Ciphers, RSA, Modes of Operations of Block Ciphers, Classical Cryptography, Modern Cryptography, Ceaser Cipher

Q2.

(i) What is IPsec? Describe about the security services provided by IPsec.

(ii) Briefly describe the following attacks;

a. DDoS

b. Spoofing

c. Man in the Middle

d. Social Engineering

(iii) Discuss about the default OS security.

(iv) How does the cultural differences effect the ethics in computer use?

Q3.

(i) Compare block ciphers and stream ciphers on their advantages over different application scenarios. Give examples

(ii) Use the permutation cipher to generate the cipher text of the following plain text.

0010010101101011100101010101010100

Key Pattern- 1-4, 2-8, 3-1, 4-5, 5-7, 6-2, 7-6, 8-3

(iii) Discuss the following statement regarding the cryptography. "They always figure out the algorithm".

(iv) Briefly describe the function of Triple DES. (use a diagram)

Q4.

(i) What are the functions of the mixing algorithm and the salt in generating KEK?

(ii) Describe the use of symmetric key cryptography and asymmetric key cryptography as hybrid cryptographic systems to share bulk data.

(iii) Discuss example scenarios we can use symmetric key cryptography and asymmetric key cryptography.

(iv) What are the mechanisms available for key recovery? Discuss their advantages and disadvantages.

Q5.

(i) What is message digest and briefly describe five (05) properties of message digest.

(ii) Describe the process of creating keyed digest and how it assure the data integrity.

(iii) How does public key cryptography address two cryptographic issues named; Nonrepudiation and Authentication using digital signature?

(iv) How do we gain unique, verifiable signature using RSA?

Q6.

(i) Describe the function of digital certificate/ public key certificate.

(ii) What are the components of PKI? Briefly describe them.

(iii) Briefly describe the two trust models used in PKI. (use diagrams)

(iv) What is certificate revocation? Describe the function of the CRL.