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

Department	**: Computer Science**
Level	**: 05**
Name of the Examination	**: Final Examination (2nd Semester)**
Course Title and - Code	**: CSU5309–Information Security and Cryptography**
Academic Year	**...: 2020/2021**

General Instructions

1. Read all instructions carefully before answering the questions.
2. This question paper consists of **06** questions in **04** 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

THE OPEN UNIVERSITY OF SRI LANKA

DEPARTMENT COMPUTER SCIENCE

B. SC. DEGREE PROGRAMME 2020/2021

FINAL EXAMINATION

CSU5309: INFORMATION SECURITY AND CRYPTOGRAPHY

DURATION: TWO HOURS (2 HOURS)

Date: 11.03.2022 **Time: 2.00 pm – 4.00 pm**

Answer **FOUR** (04) Questions **ONLY.** All questions carry equal marks.

Q1.

i. Briefly describe the following terms.

   a. Cryptology

   b. Cryptanalysis

   c. Encryption

   d. Algorithm

   e. Work factor

ii. Derive the cipher text for the following sentence for the cipher methods.

   "Active Shuttle Name is Apollo"

   a. Substitution Cipher - use encryption alphabet – EFGHIJKLMN…

   b. Caesar Cipher

   c. Transposition Cipher – key pattern 1 – 4, 2 – 8, 3 – 1, 4 – 5, 5 – 7, 6 – 2, 7 – 6, 8 – 3

iii. What is known as "breaking the algorithm"?

iv. Why it is not good to keep cryptographic algorithms secretly. Discuss by giving three reasons.

Q2.

i. Explain the one-time-pad encryption technique.

ii. What are the two ways to break PBE?

iii. Explain the function of the Trusted Third Party using a diagram.

iv. Explain the use of digital signature in verifying data transferred via electronic systems.

Q3.

i. How does the Message Digest assure the data – integrity?

ii. Explain the process of producing and verifying a DSA signature using a diagram.

iii. Briefly describe the function of the following PKI components.

a. Registration Authority
b. Certificate Directory
c. Key Recovery Server

iv. Discuss about the challenges in computer and network security implementation by covering at least three points.

Q4.

i. Name and explain the three principles used to design management controls to prevent security breaches.

ii. Briefly describe the following fundamental security design principles.

a. Economy of Mechanism
b. Open design
c. Least privilege

iii. Explain the critical characteristics of information.

iv. Compare and discuss about the two approaches used in implementing information security for an organization.

Q5.

i. Name five IPSec services at IP layer.

ii. Explain the importance of identifying following threats to an organization.

a. Power Irregularities
b. Social Engineering

c. Natural Disasters

iii. Briefly describe the ESP and AH protocol services.

iv. "Security is considered as a non-functional requirement" argue on the validity of the statement.

Q6.

i. Name five security mechanisms used to ensure physical security.

ii. Explain the following terms in relation to computational system protection mechanisms.

a. TCB

b. Principle of abstraction

c. Security labels

d. Rings

iii. What is a security perimeter? Explain with an example.

iv. By considering ten commandments of computer ethics, give three reasons to emphasize the importance of assuring information security ethics.

-End of Examination Paper –