THE OPEN UNIVERSITY OF SRILANKA
DEPARTMENT OF COMPUTER SCIENCE
B.SC.DEGREE PROGRAMME 2023/2024
FINAL EXAMINATION
CSU 5309-INFORMATION SECURITY AND CRYPTOGRAPHY
DURATION: TWO HOURS ONLY (02 HOURS)

DATE: 17.03.2024   TIME: 1.30 pm – 3.30 pm

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

Q1.

   i.   What is Computer Security?

   ii.   Describe at least four (04) fundamental Security Design Principles.

   iii.   List and briefly discuss three (3) levels of security breaches.

   iv.   List and briefly discuss three (3) key objectives of Computer Security.

(25 marks)

Q2.

   i.   State five (5) key information security concepts.

   ii.   Explain the difference between an attack surface and an attack tree.

   iii.   Briefly describe the OSI/ISO Security Architecture.

   iv.   What is the difference between a threat and an attack in Computer Security?

(25 marks)

Q3.

   i.   What is Internet Protocol Security?

   ii.   State four (04) critical characteristics of Information Security.

   iii.   Briefly describe the following attacks.

       a. Brute Force

       b. Malicious Code

       c. Spam

       d. Social Engineering

   iv.   What are the components of the Security Development lifecycle? Briefly describe.

(25 marks)

Q4.

    i.   Briefly describe the following terms.

        a. Steganography

        b. Algorithm

        c. Decipher

        d. Cryptography

    ii.   Discuss the block ciphers.

    iii. Briefly describe the function of Triple DES. (Use a diagram)

    iv. Discuss the following statement regarding cryptography. *"Why is a key Necessary? Why not create an algorithm that doesn't need a key?"*

(25 marks)

Q5.

    i.   What are the components of PKI?

    ii.   What is Stream Ciphers? Describe how stream ciphers work.

    iii. What is steganography and what can it be used for?

    iv. Briefly describe how public key cryptography works.

(25 marks)

Q6.

    i.   What is a key table? Describe how it is created and its uses.

    ii.   Describe the digital certificate.

    iii. Discuss the following statement regarding cryptography. *Why do we need a mixing algorithm?*

    iv. Explain the differences between block cipher and stream cipher.

(25 marks)

-End of Examination Paper-