RAJARATA UNIVERSITY OF SRI LANKA
FACULTY OF APPLIED SCIENCES

Bachelor of Science in Information Technology
Third Year - Semester I Examination – July / August 2023

ICT 3303 – INFORMATION SYSTEMS SECURITY

Time: Three (03) hours

Instructions

- Answer **ALL** questions.
- This paper contains **five (05)** questions in **three (03)** pages.

---

1. a) Define computer security.

(4 marks)

b) "FIPS 199 Characterization lists three security objectives for information and for information systems and provides a useful characterization of these three objectives in terms of requirements and the definition of a loss of security in each category." Give the definition of a loss of security in each of those categories.

(6 marks)

c) Explain the followings in information systems security:

i. Security policy.

ii. Vulnerability.

iii. Threat agent.

(6 marks)

d) List four (04) functional requirement areas that primarily require computer security technical measures to reduce vulnerabilities and to deal with threats to system assets in information systems.

(4 Marks)

2. a) Distinguish between a substitution cipher and a transposition cipher.

(4 marks)

b) Use the Playfair cipher to encrypt the message "Battle" with the key "Sword".

(5 marks)

c) Encrypt the paint text "INFORMATION SYSTEMS SECURITY" by using the Rail Fence cipher with depth 3.

(5 marks)

d) Briefly explain the following DES modes:

i. Cipher Block Chaining (CBC).

ii. Cipher Feedback (CFB).

(6 marks)

3. a) What are the two important characteristics of asymmetric algorithms?

(4 marks)

b) Explain how the problem of key distribution in private key encryption systems is resolved in public key encryption systems.

(4 marks)

c) In the context of public-key cryptography, briefly explain the following terms:

i. Asymmetric keys.

ii. Open message format.

iii. RSA.

(6 marks)

d) What are the three (03) broad categories of applications of public-key cryptosystems? Briefly explain them.

(6 marks)

4. a) What is PKI? List four (04) main security services provided by a PKI.

(6 marks)

b) What are the core components of a PKI? Briefly describe each component.

(6 marks)

c) Suppose that Bob receives Alice's digital certificate from someone claiming to be Alice.

i. How does Bob verify the signature on the certificate and what useful information does Bob gain by verifying the signature?

ii. After Bob verifies the signature on the certificate, what does he know about the identity of the sender of the certificate?

(4 marks)

d) Why is it not sufficient for the PKI to stop distributing a certificate after it becomes invalid?

(4 marks)

5. a) In the context of access control, briefly explain the following functional categories:

   i. Preventative access control.

   ii. Deterrent access control.

   (4 marks)

   b) Explain "Something You Have" authentication factor. Give an example.

   (5 marks)

   c) What is a cognitive password? Give an example.

   (5 marks)

   d) Briefly explain the following identification and authentication techniques:

   i. Token.

   ii. Single sign-on.

   (4 marks)

   e) Briefly explain the discretionary access control model.

   (2 marks)

--- End ---