UNIVERSITY OF RUHUNA

Faculty of Engineering

End-Semester 6 Examination in Engineering: May 2026

Module Number: EC6204 **Module Name: Information Security (C-23)**

[Two Hours]

[Answer all questions, each question carries 12.5 marks]

Q1 a) State the NIST definition of Information Security and list three categories of system resources it aims to protect.

[2 Marks]

b) State each component of the CIA Triad of NIST and describe each one in a single sentence.

[2 Marks]

c) A student intentionally alters their examination marks stored in the university database. Identify which CIA property is violated and justify in one sentence.

[2 Marks]

d) Describe how a Caesar cipher encrypts and decrypts a message.

[2 Marks]

e) State the two fundamental assumptions that cryptographers make about the communication environment and describe each in one sentence.

[2 Marks]

f) The ciphertext TFDVSJUZ was encrypted using a shift-by-1 cipher. Decrypt it and state the original plaintext.

[2.5 Marks]

Q2 a) Describe what a Feistel cipher is and state two advantages of its structure.

[2 Marks]

b) State the key difference between ECB mode and CBC mode of block cipher operation, and identify one weakness of ECB mode.

[2 Marks]

c) A bank encrypts two identical transaction records and obtains identical ciphertext blocks. Identify the cipher mode being used and state the security risk this creates.

[2 Marks]

d) State the role of a Certificate Authority (CA) in public key cryptography and explain why it is necessary.

[2 Marks]

e) Briefly describe the Diffie-Hellman key exchange protocol and state the security problem it solves.

[2 Marks]

f) Bob claims he received a digitally signed purchase order from Alice. Alice denies sending it. Examine which security property is relevant and explain how digital signatures resolve this dispute.

[2.5 Marks]

Q3 a) List four properties of a good cryptographic hash function and describe each in one sentence.

[2 Marks]

b) State the primary security goal of cryptography and the primary security goal of steganography, and briefly explain the key difference between them.

[2 Marks]

c) A website stores user passwords as plain text, and all passwords are exposed during a breach. Choose one security measure that should have been implemented and briefly explain its benefit.

[2 Marks]

d) State the difference between authentication and authorization and give one example of each.

[2 Marks]

e) State the Simple Security Property (no-read-up) of the Bell-LaPadula model and briefly explain its rationale.

[2 Marks]

f) A firm's clerk attempts to access the HR manager's confidential salary records. State whether this should be permitted under the Bell-LaPadula model and justify your answer.

[2.5 Marks]

Q4 a) List four distinct types of malware and describe each in one sentence.

[2 Marks]

b) State the difference between a signature-based IDS and an anomaly-based IDS. Include one advantage and one limitation of each.

[2 Marks]

c) A worm modifies its own decryption module after each replication to avoid detection. Identify the specific type of malware and briefly explain why signature-based detection fails.

[2 Marks]

d) Define non-repudiation and briefly explain why it is a critical requirement in digital communications.

[2 Marks]

e) Briefly describe one scenario where ECC is more suitable than RSA and state the key advantage ECC offers in that scenario.

[2 Marks]

f) Alice uses a MAC to authenticate a stock purchase from her broker Bob. Bob later denies receiving the order. State whether the MAC can prevent Bob's denial and what should have been used instead.

[2.5 Marks]