

QP CODE 2010558101

Reg. No

--	--	--	--	--	--	--	--	--	--



DMI-ST. EUGENE UNIVERSITY

ZAMBIA

DEGREE EXAMINATION – DECEMBER 2024

Semester: X 055EL003 INFORMATION SECURITY

Time: 3:00 Hours

Max. Marks: 100

Answer any FIVE Questions (5 x 20 = 100 Marks)

1. a) Discuss in detail the various types of attacks in network security. Provide suitable examples to support your explanation. **(10 Marks)**
b) Explain the fundamental security services in network security. **(5 Marks)**
c) Explain the need for security in modern computing systems and networks. Discuss the core principles of security and how they contribute to the protection of information. **(5 Marks)**
2. a) Describe the concept of confidentiality in symmetric encryption. Explain how traffic confidentiality is achieved using symmetric encryption. Provide a detailed example of a symmetric encryption scheme and discuss its application in securing data during transmission. **(10 Marks)**
b) Explain the role of key distribution in symmetric encryption. Why is it crucial for maintaining the confidentiality of encrypted data? **(5 Marks)**
c) What is the significance of random number generation in symmetric encryption? Briefly describe how random numbers are used in the encryption process. **(5 Marks)**
3. a) Discuss the concept of message authentication. Explain the various authentication functions and codes used to verify message integrity and authenticity. Provide examples. **(10 Marks)**
b) Define hash functions and explain their role in ensuring data integrity. **(5 Marks)**
c) List and briefly describe three hash algorithms. **(5 Marks)**
4. a) Explain the working of the Kerberos authentication protocol. How does it ensure secure communication between two parties? Illustrate the key steps involved in the authentication process. **(10 Marks)**

- b) Describe the purpose and benefits of S/MIME in securing email communication. **(5 Marks)**
 - c) What is the role of the Authentication Header (AH) in IP security? How does it ensure data integrity and authenticity? **(5 Marks)**
- 5.
- a) Explain the differences between Secure Socket Layer (SSL) and Transport Layer Security (TLS). How do these protocols ensure secure communication over the web? **(10 Marks)**
 - b) Discuss the role of firewalls in network security. What are the key design principles of a secure firewall? **(5 Marks)**
 - c) What is a Virtual Private Network (VPN)? Explain how it ensures secure communication over public networks. **(5 Marks)**
- 6.
- a) Explain the concept of digital signatures. How do they enhance security in communication? Include an example of a digital signature process. **(10 Marks)**
 - b) What are authentication protocols? Give one example and explain their use. **(5 Marks)**
 - c) What is the Digital Signature Standard (DSS)? Briefly describe its purpose and application. **(5 Marks)**
- 7.
- a) Discuss the importance of trusted systems in ensuring the security of critical data. How do trusted systems contribute to overall network security? **(10 Marks)**
 - b) Explain the function of Intrusion Detection Systems (IDS) and how they help detect and prevent attacks. Include examples of signature-based and anomaly-based detection methods. **(10 Marks)**