

# PURBANCHAL UNIVERSITY

2025

Bachelor in Information Technology (B.I.T.)/Fifth Semester/ *Final*

Time: 03:00 hrs.

Full Marks: 60 /Pass Marks: 24

**BIT303CO: Cryptography and Network Security (New)**

*Candidates are required to give their answers in their own words as far as practicable. The figures in the margin indicate full marks.*

## Group A

**Answer TWO questions.**

**2×12=24**

1. What do you mean by asymmetric key cryptography? Explain about Data Encryption Standard (DES) with its suitable architecture and explain its working principle in details. 2+10
2. Define Security Electronic Transaction (SET) and SSL. Explain the architecture of SSL with suitable block diagram. 4+8
3. What is WAP and what is its primary purpose in mobile networking? How does WAP ensure secure communication and what are the challenges of implementing end-to end security in WAP networks? 4+8

## Group B

**Answer SIX questions.**

**6×6=36**

4. Differentiate between network security, information security and cyber security.
5. What is an IP address and why is it essential? Write the differences between hub, switch and router. 3+5
6. What are the basic objectives of information security? Explain CIA security model. 2+6
7. What is the primary objective of IPSec? Briefly explain the components of IPSec. 2+6
8. Why do we need TLS? Explain the working principle of TLS.
9. Define threat, attack and vulnerability. Explain about the threats to information security. 3+5
10. What is the purpose of Intrusion Detection System (IDS)? Write the differences between network-based IDS and host-based IDS.
11. Define play fair cipher algorithm. Encrypt the following plain text into cipher text by using play fair cipher algorithm.

Key: NETWORK

Plain Text: PURBANCHAL UNIVERSITY

[2+6]

**Contd. ...**



(2)

12. Write short notes on Any TWO:
- (a) Intrusion prevention system
  - (b) RSA algorithm
  - (c) Wireless transport layer security

