TRIBHUVAN UNIVERSITY
FACULTY OF MANAGEMENT
Office of the Dean
2016

Full Marks: 60
Time: 3 hrs

BIM/Eighth Semester/ ITC 229 : Computer Security and Cyber Law

Candidates are required to answer the questions in their own words as far as practicable

Group "A"

1. Brief Answer Question: **[10×1=10]**

- **i.** Differentiate between security and safety.
- **ii.** What do you mean by one time pad?
- **iii.** How does block cipher differ from stream cipher?
- **iv.** Define e-government.
- **v.** List the threats that are enabled by E-mail.
- **vi.** Define security evaluation criteria.
- **vii.** Differentiate between computer and network security.
- **viii.** How does digital forensics differ from computer security?
- **ix.** Why passive attacks are difficult to detect?
- **x.** List the differences between password guessing and password capture.

Group "B"

Short Answer Question: **[6×5=30]**

2. Define Asymmetric key cryptography. In asymmetric key cryptography system using RSA, you intercepted the cipher text C= 4 sent to user whose public key e = 5 and n= 39. Find the plain text M.

3. Explain any three common securities related programming problem in short.

4. Define web security. Explain SSL Handshake in brief.

5. Explain the function of different DMZ servers.

6. List the difference between open source and proprietary software. Explain any three general security rule.

7. Write short notes on:
- **a.** Intellectual property.
- **b.** IDS architecture.

Group "C"

Long Answer Question: **[2×10=20]**

8. Define malicious logic and explain its type. Explain various defense mechanism of malicious logic

9. Why is digital signature used? Explain different digital signature standards in brief.